On lexicographic Gröbner bases of radical ideals in dimension zero: interpolation and structure

X. Dahan[1]

Faculty of Mathematics, Kyûshû university, Fukuoka Japan

Abstract

Due to the elimination property held by the lexicographic monomial order, the corresponding Gröbner bases display strong structural properties from which meaningful informations can easily be extracted. We study these properties for radical ideals of (co)dimension zero. The proof presented relies on a combinatorial decomposition of the finite set of points whereby iterated Lagrange interpolation formulas permit to reconstruct a minimal Gröbner basis. This is the first fully explicit interpolation formula for polynomials forming a lexicographic Gröbner basis, from which the structure property can easily be read off. The inductive nature of the proof also yield a triangular decomposition algorithm from the Gröbner basis.

Keywords: Gröbner basis, Lexicographic order, Interpolation

1. Introduction

Generalities. The lexicographic monomial order benefits fully of the *elimination property*, implying a lot of structure in the polynomials of such Gröbner bases. Concretely, for "non-generic" Gröbner bases, some common factors are repeated among several polynomials, inducing some redundancies. "Non-generic" implies here Gröbner bases which have more polynomials than the number of variables. These redundancies explain why they are often huge, quite impracticable for substantial computations (as compared to the degree reverse lexicographic order in particular). On the other hand, this structure makes easy the extraction of meaningful informations. For instance, an early application was the possibility to solve polynomial systems [3, Method 6.10] [12] in the case where the number of solutions is finite (that is when the generated ideal is of *(co)dimension zero*, as we will rather say hereafter). The structure is also useful to express the polynomials in such Gröbner bases with interpolation formulas, in function of the solution points. Such formulas allow to get reasonably sharp upper bounds on the size of coefficients, as it was achieved for some special cases of lexicographic Gröbner bases in [7, 8, 6]. Another application is the possibility to decompose such "non-generic" Gröbner bases into smaller ones. This principle fits the realm of *triangular decompositions*, and the fact that starting to decompose from a lex. G.b. is easier is due to Lazard [14, Section 5]. He sketched two methods to perform this decomposition, and claimed correctness resorting to Gianni-Kalkbrener's theorem [12, 10]. But with no more details, and it appears not obvious whether this is sufficient. Probably not, indeed a proof becomes easy when resorting to the stronger Theorem (structure) provided here. More details on this is found in the paragraph *Specialization...* below.

Email address: dahan@math.kyushu-u.ac.jp (X. Dahan)

[1]Supported by the GCOE program "Math-for-Industry" of Kyûshû university

Structure theorem. Let k be a field, $k[X_1, \ldots, X_n]$ the polynomial ring with n variables on which is put the lexicographic monomial order $\preccurlyeq$ for which $X_1 \preccurlyeq X_2 \preccurlyeq \cdots \preccurlyeq X_n$ and $I \subset k[X_1, \ldots, X_n]$ a radical ideal of dimension zero (its associated prime ideals are all maximal). In this case the degree $d(I)$ of I is the finite integer equal to $\dim_k k[X_1, \ldots, X_n]/I$.

(H) Assume that k is infinite, or else that $d(I) < |k|$. Moreover, if k is of finite characteristic, for each associated prime ideal $\mathfrak{m}$ to I, the finite field extension $k \,|\, k[X_1, \ldots, X_n]/\mathfrak{m}$ is separable (this is always the case if k is a finite field).

Let $V \subset \overline{k}^n$ be the set of common zeroes of the polynomials in I, with coordinates taken in the algebraic closure $\overline{k}$ of k. Because of the separability assumption **(H)** above, the cardinal of V is equal to $d(I)$.

Let $\mathcal{G}$ be a lexicographic Gröbner basis of I. We assume that it is minimal, that is $\textsc{lm}(\mathcal{G})$ is a minimal monomial basis for the monomial ideal $\langle \textsc{lm}(I) \rangle$. But we do not necessarily assume that $\mathcal{G}$ is reduced. Since the polynomial ring is over a field k, it does not matter to require $\mathcal{G}$ to be *monic*: all the polynomials in $\mathcal{G}$ have a leading coefficient equal to 1. For $1 \leq i \leq n-1$, let $R_i := k[X_1, \ldots, X_i]$. Given a polynomial $f \in k[X_1, \ldots, X_n]$, let $\textsc{lc}_i(f) \in R_i$ be the leading coefficient of $f \in R_i[X_{i+1}, \ldots, X_n]$. Furthermore, $\textsc{lt}_i(f)$ and $\textsc{lm}_i(f) \in k[X_{i+1}, \ldots, X_n]$ will denote respectively the leading term and the leading monomial of $f \in R_i[X_{i+1}, \ldots, X_n]$ yielding the equality $\textsc{lt}_i(f) = \textsc{lc}_i(f)\textsc{lm}_i(f)$.

Theorem (Structure). *For all $g \in \mathcal{G}$, $g \notin k[X_1, \ldots, X_{n-1}]$, holds:*

$$g \in \langle \textsc{lc}_1(g) \rangle \quad (\iff \textsc{lc}_1(g) \,|\, g) \ , \quad \forall 2 \leq t \leq n-1, \quad g \in \langle \textsc{lc}_t(g) \rangle + I_{t-1}.$$

$$\textit{Moreover,} \qquad \forall t' > t \qquad \textit{holds} \qquad \textsc{lc}_{t'}(g) \in \langle \textsc{lc}_t(g) \rangle + I_{t-1}.$$

This structure theorem has a direct application in the context of *specialization* of Gröbner bases. The proof of this theorem is easily reduced to show the existence of *one* Gröbner basis which verifies these properties.

Theorem (Interpolation). *Let V denotes the set of common zeroes of the polynomials in I. There is a combinatorial decomposition of V which allows to describe each polynomial $g \in \mathcal{F}$ as explicit interpolation formulas (Corollary 2 and Equation* (28)*).*

The structure theorem already appear in a work of Marinari-Mora [16]. They even managed to generalize it to slightly more general ideals than radical ones in [17]. Note that the formulation given therein is slightly different, but the above is more handy. However, some novelty is brought in, as detailed hereunder:

1. The proof in [16, 17] is *quite* unwieldy, making it difficult to check correctness. It is build upon the combinatorial algorithm of Cerlienco-Mureddu [5] to deduce the leading monomials of minimal Gröbner bases of I. More recently a more suited combinatorial algorithm "lex game" [9] has appeared, which is also more efficient (see discussion in § 3 therein). Our presentation of the decomposition algorithm in § 3 is quite similar, but is simplified and the proof is different and more rigorous.
2. based on the decomposition of § 3 we give new explicit interpolation formulas. These are well-suited to generalize the use of *fast interpolation* algorithms, and to derive a good running-time for the reconstruction algorithm. These explicit formulas are also *necessary* to obtain complexity estimates on the size of coefficients by using *height theory* as done in [8, 6].
3. a main new ingredient of the present article is the recursive point of view of the proof of Theorem 3. Besides its conceptual simplicity regarding the other previous works, it prepares the ground for a first proof of the algorithm `lextriangular` (mentioned above).

Previous work. As already said, there is a variety of previous works dealing more or less closely with the same kind of results. A comparison with [16, 17] has been discussed in 1. above. On the more specific part concerning interpolation there are also several previous works. Let us mention the most recent one [15]. It describes an algorithm to compute the reduced Gröbner basis of the ideal of vanishing polynomials on a Zariski-closed finite set. It claims (no discussion about running-times is provided) to subsume the earlier but more general Buchberger-Möller algorithm [4]. The highlight of his proof is the use of an operation on standard monomials, with well-suited Lagrange interpolation. It is therefore rigorous but no explicit interpolation formula is supplied and thus deriving the structure theorem is not obvious. Indeed, it is thanks to the explicit formulas that the proof of Theorem (Structure) is quite straightforward. On the other hand, in order to describe these formulas, we introduce a combinatorial decomposition of the zero-set V which is quite technical to define.

This combinatorial decomposition is very similar to the one appearing in the "lex game" [9]. The purpose therein is to find the set of standard monomials of a finite set of points in the n-affine space. The present work is going further with the addition of interpolation to describe the Gröbner basis, while in the same purely combinatorial manner only the set of standard monomials can also be deduced. The recursive proof given is also different and has the advantage to prepare the ground for the `lextriangular`algorithm. Moreover, we have tried to reduce the number of notations as low as possible and to present the decomposition as plain as possible. This was thought in the hope to provide with this more suited decomposition than the Cerlienco-Mureddu [5], a more rigorous and easy to read proof of the Theorem (Structure) than [16, 17], which is also a contribution of this work.

In comparison with [15, 9], the present article provides a similar combinatorial decomposition of § 3 as the one provided by the "lex-game" (see § 2.3 therein) but has the additional benefits mentioned in 2.-3. above, which are *necessary* to pursue the works on complexity and on `lextriangular`. Moreover, the interpolation part of § 4 is more explicit, with the possibility to provide a good running-time, improving upon possibly the algorithm of [15].

Concerning the structure theorem, before this theorem was stated in [16], previous works on the structure have been considered. In the easy case of a polynomial ring with two variables, Lazard has found out that the structure theorem hold for any ideal, not only radical one [13].

Theorem (D. Lazard). *Let $J \subset k[X_1, X_2]$ be a zero-dimensional ideal, and $f_1, \ldots, f_r$ a minimal lexicographic Gröbner basis of J for $X_1 \preccurlyeq_{lex} X_2$. Then:*

$$\mathrm{LC}_1(f_i) \in k[X_1] \quad \textit{divides} \quad \mathrm{LC}_1(f_j) \textit{ for all } \quad i \geq j,$$

$$\textit{and} \quad \mathrm{LC}_1(f_i) \quad \textit{divides} \quad f_i \quad \textit{as well.}$$

It follows easily a factorization property of the polynomials in such a Gröbner basis, which is actually the original statement[2] of Lazard [13, Theorem 1 (i)]. In the case of a radical ideal this is equivalent to Theorem (Structure) aforementioned. Note that if I is not radical, Theorem (Structure) does not hold for $n > 2$.

Then Gianni and Kalkbrener [10, 12] independently presented a form of structure theorem stated in the context of specialization of Gröbner bases.

Application to stability of Gröbner bases under specialization. The stability of a Gröbner basis under a homomorphism map goes beyond the scope of this article (see [1] for details). When

[2]However, the formulation above is more compact and handy, and is equivalent assuming that we are considering only minimal and monic Gröbner bases.

the homomorphism map ϕ is a *specialization* and takes the following form: for $1 \leq \ell \leq n-1$ and $(\alpha_1, \ldots, \alpha_\ell) \in \overline{k}^\ell$,

$$\begin{array}{rcl} \phi : \overline{k}[X_1, \ldots, X_n] & \longrightarrow & \overline{k}[X_{\ell+1}, \ldots, X_n] \\ P(X_1, \ldots, X_n) & \longmapsto & P(\alpha_1, \ldots, \alpha_\ell, X_{\ell+1}, \ldots, X_n), \end{array}$$

then given a monomial order $\preccurlyeq_\ell$ that eliminates the variables $X_1, \ldots, X_\ell$, $I \subset k[X_1, \ldots, X_n]$ is said to be *stable* under ϕ if and only if: $\phi(\mathrm{LT}_\ell(I)) = \mathrm{LT}(\phi(I))$ (only the inclusion $\supset$ is not automatically satisfied). Hence, if G is a Gröbner basis of I this implies that $\phi(G)$ is a Gröbner basis of $\phi(I)$. It may happen though that $\phi(G)$ is a Gröbner basis of $\langle \phi(G) \rangle \subset \overline{k}[X_{\ell+1}, \ldots, X_n]$ without verifying $\langle \phi(G) \rangle = \phi(I)$ [10, Rmk 2, Ex. 3]. If the monomial order is lexicographic and I is radical of dimension zero as in Hypothesis (H), then Theorem (Structure) applies and implies stability. More precisely:

Corollary 1. *With the notations and assumptions above, given a minimal Göbner basis $\mathcal{G}$ of I, and $g \in \mathcal{G}$, the following equivalence holds:*

$$\phi(\mathrm{LT}_\ell(g)) = 0 \iff \phi(g) = 0.$$

In particular, $\mathrm{LT}(\phi(g)) = \phi(\mathrm{LT}_\ell(g))$ *and the stability property holds. Hence $\phi(\mathcal{G})$ is a Gröbner basis of $\phi(I)$.*

It is noteworthy that Becker in [2] proves that $\phi(G)$ remains a Gröbner basis but he does not prove stability[3], letting unproved the fact that $\langle \phi(G) \rangle = \phi(I)$.

When all the variables but the largest are specialized, that is when $\ell = n-1$, Gianni-Kalkbrener [10, 12] has proved that in the case of a radical ideal I, the stability property holds. It strongly relies on Lemma 5.6 of [11]. As shows Corollary 1, Theorem (Structure) is the genuine generalization of Gianni-Kalkbrener (which is not the result of Becker [2]).

Organization of the paper. In § 2 hereunder we treat the case $n = 3$ to keep up a geometric intuition. The other sections § 3-4-5 aim at generalizing to more than 3 variables. § 3 introduces the combinatorial decomposition of the set of points that determines the leading terms of the minimal Gröbner basis. § 4-5 are proving this fact by constructing explicitly polynomials by interpolation (§ 4), which are proved in § 5 to form a Gröbner basis.

2. Warming-up: case of three variables

The first case for which difficulties arise is when $n = 3$. The case $n = 2$ is too special to reveal any genuine technical problem. Though, the way to combine a decomposition of the zero set and Lagrange interpolation formula appears in [6, § 2.2][4] which we are trying to generalize here to the case of three variables.

2.1. Set-up

The notations hereunder are not restricted to the case $n = 3$ and will be used all along the paper.

[3] his proof can not be adapted. In the proof of the crucial Lemma 1, in Equality (4) is assumed a degree decrease that prevents to consider stability.

[4] as a matter of facts, the use of the *equiprojectable decomposition* becomes obsolete for $n > 2$

Notations. Given an n-uplet $y = (y_1, \ldots, y_n)$ and an $1 \leq \ell \leq n-1$ let π_ℓ be the projection that forgets the last $n - \ell + 1$ coordinates: $\pi_\ell(y) = (y_1, \ldots, y_\ell)$. And let $p_\ell(y) = y_\ell$ be the ℓ-th coordinate function. Given another integer ℓ' such that $\ell < \ell' \leq n$, define $p_{\ell,\ell'}(y) := (y_\ell, \ldots, y_{\ell'})$. Fibers of projection maps are used intensively and it is convenient to precise the length of the starting sequence: $\pi_{\ell',\ell}$ denotes the projection $\pi_{\ell',\ell}(y_1, \ldots, y'_\ell) = (y_1, \ldots, y_\ell)$, The point of this notation is when taking reciprocal images $\pi^{-1}_{\ell',\ell}(\,\cdot\,)$ to know the dimension of the starting space.

Given a set $S \subset \overline{k}^\ell$, and $\alpha \in \overline{k}^{\ell-1}$ for we introduce a convenient notation $S[\alpha]$:

$$\begin{array}{rcll} S : \overline{k}^{\ell-1} & \longrightarrow & \mathcal{P}(\overline{k}^\ell) & (\textit{set of parts of } \overline{k}^\ell) \\ \alpha & \longmapsto & S[\alpha] := \pi^{-1}_{\ell,\ell-1}(\{\alpha\}) \cap S & \end{array} \tag{1}$$

The proofs in this paper deal a lot with minimal bases of monomial ideals for a which a special notation is necessary:

Definition 1. *Given an ideal $I \subset k[X_1, \ldots, X_n]$, $\min(I)$ will denote the minimal basis of the monomial ideal $\langle \textsc{lm}(I) \rangle$.*

If $\mathcal{G}$ is a minimal Gröbner basis of I, then $\{\textsc{lm}(g) \mid g \in \mathcal{G}\}$.

Case n=2. First, let us briefly review how the case $W \subset \overline{k}^n$ Zariski-closed over k, works for $n = 2$. The ideal $I(W)$ of vanishing polynomials on W is denoted J, and the goal is to determine the minimal basis $\min(J)$ of $\langle \textsc{lm}(J) \rangle$.

- X_1^a is in the minimal basis, where $a := |\pi_1(W)|$.
- $X_1^c X_2^d$ is in the monomial basis if and only if $W^d := \{y = (y_1, y_2) \in W \mid |\pi_1^{-1}(y_1) \cap W| = d\}$ is not empty, *and* $|\pi_1(\cup_{\ell > d} W^\ell)| = c$.

The proof in [6] builds explicitly a Gröbner basis from W to prove these assertions. Let us carry through the case $n = 3$.

Strategy. Let $V \subset \overline{k}^3$, Zariski-closed over k. The ideal $I(V)$ of vanishing polynomials on V is denoted I. The strategy can be summarized as follows:

1. to each couple of integers $(i_2, i_3) \in \mathbb{N}^2$, associate "naturally" a subset $\widetilde{V}^{i_3,i_2}$ that may be empty. If it is not, this determines a third integer i_1 and $X_1^{i_1} X_2^{i_2} X_3^{i_3} \in \min(I)$.
2. construct by interpolation a polynomial that vanishes on V and that has $X_1^{i_1} X_2^{i_2} X_3^{i_3}$ for leading monomial.
3. prove that $\min(I)$ is equal to $\min(I \cap k[X_1, X_2])$ union the $X_1^{i_1} X_2^{i_2} X_3^{i_3}$ for each 3-uplets (i_1, i_2, i_3) mentioned in 1.

As it stands in this paper, the constructed Gröbner basis is not reduced. Experimentally, it has however smaller coefficients (proved in the case of 2 variables in [6]).

2.2. Decomposition

Let $V^\ell := \{y \in V \mid |\pi^{-1}_{3,2}(y_1, y_2) \cap V| = \ell\} = \{y \in V \mid |V[\alpha]| = \ell\}$. It is clear that it defines a partition of V and since V is finite, that almost all V^ℓ are empty. Let i_3 be such that $V^{i_3} \neq \emptyset$. The shortcut notations $V^{\leq i_3} := \cup_{\ell \leq i_3} V^\ell$ and $V^{>i_3} = \cup_{\ell > i_3} V^\ell$ will be convenient. Let $S'_2 := \pi_2(V^{>i_3})$ and $S_2 := \pi_2(V^{\leq i_3})$.

Lemma 1. *$\pi_2(V) = S_2 \cup S'_2$ and $S_2 \cap S'_2 = \emptyset$.*

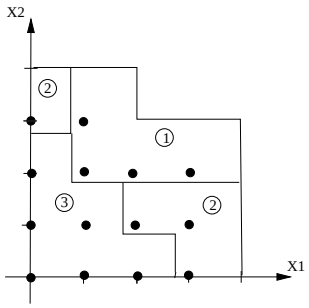

Figure 1: Set of points in $\mathbb{Q}^3$

PROOF. Given $(y_1, y_2) \in S_2$, there exists $y_3 \in \overline{k}$ such that $(y_1, y_2, y_3) \in V^{\leq i_3}$. Thus $|\pi_{3,2}^{-1}(y_1, y_2) \cap V| \leq i_3$, whereas if $(x_1, x_2) \in S_2'$, then $|\pi_{3,2}^{-1}(x_1, x_2) \cap V| > i_3$. This shows that $S_2 \cap S_2' = \emptyset$. Since $V = V^{>i_3} \cup V^{\leq i_3}$, holds $\pi_2(V) = S_2 \cup S_2'$.

Note that S_2 and S_2' depends on i_3. For the next step, let us introduce for $\ell \in \mathbb{N}$:

$$V^{i_3,\ell} := \{y = (y_1, y_2, y_3) \in V \mid |\pi_{2,1}^{-1}(y_1) \cap S_2| = \ell\} \quad (2)$$

$$\widetilde{V}^{i_3,\ell} := \{y = (y_1, y_2, y_3) \in V^{i_3} \mid |\pi_{2,1}^{-1}(y_1) \cap S_2| = \ell\} = V^{i_3,\ell} \cap V^{i_3}. \quad (3)$$

Again it is clear that $(V^{i_3,\ell})_{\ell \in \mathbb{N}}$ is a partition of V, and that almost all $V^{i_3,\ell}$ are empty. Thus, $(\widetilde{V}^{i_3,\ell})_{\ell \in \mathbb{N}}$ is a partition of V^{i_3} and almost all $\widetilde{V}^{i_3,\ell}$ are empty. Let i_2 be such that $\widetilde{V}^{i_3,i_2}$ is not empty, and let $V^{i_3,\leq i_2} := \cup_{\ell \leq i_2} V^{i_3,\ell}$ while $V^{i_3,>i_2} := \cup_{\ell > i_2} V^{i_3,\ell}$. Finally let $S_1' := \pi_1(V^{i_3,>i_2})$ and $S_1 := \pi_1(V^{i_3,\leq i_2})$ and define $i_1 := |S_1'|$.

Lemma 2. *$\pi_1(V) = S_1 \cup S_1'$ and $S_1 \cap S_1' = \emptyset$*

PROOF. The first equality directly results from the fact that $V = V^{i_3,>i_2} \cup V^{i_3,\leq i_2}$. As for the second, if $y_1 \in S_1$ then $|\pi_{2,1}^{-1}(y_1) \cap S_2| \leq i_2$ whereas $x_1 \in S_1'$ must fulfill $|\pi_{2,1}^{-1}(y_1) \cap S_2| > i_2$.

The insight of the decomposition is that $X_1^{i_1} X_2^{i_2} X_3^{i_3}$ is in the monomial basis $\min(I)$ of $\langle \text{LM}(I) \rangle$. Let $\mathcal{L}(\widetilde{V})$ and $\mathcal{L}'(\widetilde{V})$ be the sets:

$$\mathcal{L}(\widetilde{V}) := \{(i_2, i_3) \in \mathbb{N}^2 \mid \widetilde{V}^{i_3,i_2} \neq \emptyset\}. \quad (4)$$

$$\mathcal{L}'(\widetilde{V}) := \{(i_1, i_2, i_3) \in \mathbb{N}^3 \mid (i_2, i_3) \in \mathcal{L}(\widetilde{V}) \text{ and } i_1 = |\pi_1(V^{i_3,>i_2})| = |S_1'|\}. \quad (5)$$

Let us illustrate how the decomposition works on an oversimplified but eloquent enough example.

Example. Consider the finite set of points $V \subset \mathbb{Z}^3 \subset \overline{\mathbb{Q}}^3$ described hereafter. Define $\pi_1(V) := \{0, 1, 2, 3, 4, 5\}$, and $\pi_2(V)$ the points $\bullet$, having integer coordinates in Figure 1.

The third coordinate of the points in V is determined by the circled number inside the regions delimited by Figure 1. For example the point of coordinate $(0, 0)$ is inside the region marked 3, hence determines a point $(0, 0, 3) \in V$. The point with coordinates $(3, 1)$ is inside the region marked 2, hence the three coordinates are $(3, 1, 2)$. The cardinality of V is $|V| = 3.6+2.4+1.4 = 28$. The regions delimited in Figure 1 illustrates the decomposition $V = V^1 \cup V^2 \cup V^3$ defined at the beginning of § 2.2.

Let us fix $i_3 = 2$. Then Figure 2 illustrates the decomposition $V = V^{i_3,0} \cup V^{i_3,1} \cup V^{i_3,2} \cup V^{i_3,3}$ defined in Equation (2).

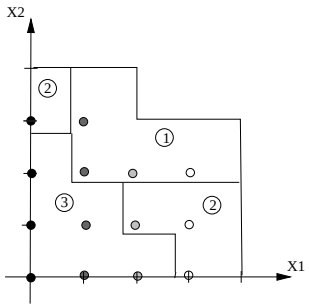

Figure 2: Black $\to V^{2,3}$. Grey: $\to V^{2,2}$. Light gray: $\to V^{2,1}$. White $\to V^{2,0}$

2.3. Interpolation

Lagrange interpolation. The decomposition above permits to set up Lagrange interpolation formulas. We recall the basics along with setting notations.

Given a finite set U of points in $\overline{k}$, Zariski-closed over k and of cardinal $|U| = u$, the *Lagrange basis on U* of the u-dimensional k-vector space $k[x]_{<u}$ is defined as:

$$\{\ell_\alpha(x)\}_{\alpha\in U} \quad \text{where} \quad \ell_\alpha(x) := \prod_{\substack{\beta\in U\\ \beta\neq\alpha}} \frac{x-\beta}{\alpha-\beta}. \tag{6}$$

An element $P \in k[x]_{<u}$ is written in this basis $P(x) = \sum_{\alpha\in U} P(\alpha)\ell_\alpha(x)$, in particular:

$$1 = \sum_{\alpha\in U} \ell_\alpha(x). \tag{7}$$

Formula. With the notations of the § 2.1, given $\mathbf{i} = (i_2, i_3)$ such that $\widetilde{V}^{i_3,i_2} \neq \emptyset$ define:

$$g_{\mathbf{i}} := \left(\prod_{\alpha'\in S_1'} X_1 - \alpha'\right)\left\{\sum_{\alpha\in S_1} \ell_\alpha(X_1) X_2^{i_2-|S_2'[\alpha]|}\left(\prod_{\beta'\in S_2'[\alpha]} X_2 - \beta_2'\right)\left[\sum_{\beta\in S_2[\alpha]} \ell_{\beta_2}(X_2) X_3^{i_3-|V[\beta]|}\left(\prod_{\gamma\in V[\beta]} X_3 - \gamma_3\right)\right]\right\} \tag{8}$$

The following Proposition contains the conclusion of Theorem (structure) of the introduction.

Proposition 1. *Defining $i_1 := |S_1'|$, the leading monomial of $g_{\mathbf{i}}$ is $X_1^{i_1}X_2^{i_2}X_3^{i_3}$.*
Moreover, define g_1 as the unique monic polynomial such that $I_1 := I \cap k[X_1] = \langle g_1\rangle$. Then, $\mathrm{LC}_1(g_{\mathbf{i}})$ divides $g_{\mathbf{i}}$ and $g_{\mathbf{i}} \in \langle \mathrm{LC}_2(g_{\mathbf{i}}), g_1\rangle = \langle g_1\rangle = \langle \mathrm{LC}_2(g_{\mathbf{i}}) + I_1$.

Proof. The degree in X_3 of the polynomials $X_3^{i_3-|V[\beta]|}\left(\prod_{\gamma\in V[\beta]} X_3 - \gamma_3\right)$ are equal to i_3 for all $\beta \in S_2[\alpha]$ and for all $\alpha \in S_1$. Because $1 = \sum_{\beta\in S_2[\alpha]} \ell_{\beta_2}(X_2)$, and hence $X_3^{i_3} = \sum_{\beta\in S_2[\alpha]} \ell_{\beta_2}(X_2)X_3^{i_3}$, it follows that the leading monomial of the polynomial

$$f_\alpha(X_2, X_3) := \sum_{\beta\in S_2[\alpha]} \ell_{\beta_2}(X_2) X_3^{i_3-|V[\beta]|}\left(\prod_{\gamma\in V[\beta]} X_3 - \gamma_3\right), \tag{9}$$

is $X_3^{i_3} = \mathrm{LM}(f_\alpha)$, for all $\alpha \in S_1$.

Similarly, the degree in X_2 of all the polynomials $X_2^{i_2-|S_2'[\alpha]|}\left(\prod_{\beta'\in S_2'[\alpha]} X_2-\beta_2'\right)$ is i_2, yielding:

$$\textsc{lm}\left(X_2^{i_2-|S_2'[\alpha]|}\left(\prod_{\beta'\in S_2'[\alpha]} X_2-\beta_2'\right) f_\alpha(X_2,X_3)\right)=X_2^{i_2}X_3^{i_3}. \tag{10}$$

It follows that $g_{\mathbf{i}}=\left(\prod_{\alpha'\in S_1'} X_1-\alpha\right)\left(\sum_{\alpha\in S_1}\ell_\alpha(X_1)(X_2^{i_2}X_3^{i_3}+\cdots)\right)$. By Equation (7), because $X_2^{i_2}X_3^{i_3}=\sum_{\alpha\in S_1}\ell_\alpha(X_1)X_2^{i_2}X_3^{i_3}$, $g_{\mathbf{i}}$ verifies $g_{\mathbf{i}}=\left(\prod_{\alpha'\in S_1'} X_1-\alpha\right)(X_2^{i_2}X_3^{i_3}+\cdots)$. By definition of i_1 equal to the cardinal of S_1', one gets $\textsc{lm}(g_{\mathbf{i}})=X_1^{i_1}X_2^{i_2}X_3^{i_3}$.

Equation (8) clearly shows that $\textsc{lc}_1(g_{\mathbf{i}})=\prod_{\alpha\in S_1'} X_1-\alpha$ divides $g_{\mathbf{i}}$. Let $\alpha\in S_1$. Then $\frac{g_{\mathbf{i}}}{\textsc{lc}_1(g_{\mathbf{i}})}(\alpha,X_2,X_3)=X_2^{i_2-|S_2'[\alpha]|}\left(\prod_{\beta'\in S_2'[\alpha]} X_2-\beta_2'\right) f_\alpha(X_2,X_3)$ and one sees that

$$\textsc{lc}_2\left(\frac{g_{\mathbf{i}}}{\textsc{lc}_1(g_{\mathbf{i}})}(\alpha,X_2,X_3)\right)\quad\text{divides}\quad\frac{g_{\mathbf{i}}}{\textsc{lc}_1(g_{\mathbf{i}})}(\alpha,X_2,X_3).$$

The Chinese Remaindering Theorem implies that $\textsc{lc}_2(\frac{g_{\mathbf{i}}}{\textsc{lc}_1(g_{\mathbf{i}})})$ divides $\frac{g_{\mathbf{i}}}{\textsc{lc}_1(g_{\mathbf{i}})}$ modulo $\frac{g_1}{\textsc{lc}_1(g_{\mathbf{i}})}$, hence that $g_{\mathbf{i}}\in\langle\textsc{lc}_2(g_{\mathbf{i}}),g_1\rangle$.

Lemma 3. *The polynomial $g_{\mathbf{i}}$ vanishes on V.*

Proof. First, the factor $\textsc{lc}_1(g_{\mathbf{i}})=\prod_{\alpha\in S_1'} X_1-\alpha'$ implies that $g_{\mathbf{i}}$ vanishes on $V^{i_3,>i_2}$, since $S_1'=\pi_1(V^{i_3,>i_2})$. Because $V=V^{i_3,>i_2}\cup V^{i_3,\leq i_2}$, it remains to show that $\widetilde{g_{\mathbf{i}}}:=\frac{g_{\mathbf{i}}}{\textsc{lc}_1(g_{\mathbf{i}})}$ vanishes on $V^{i_3,\leq i_2}$.

For $\alpha\in S_1$, $\widetilde{g_{\mathbf{i}}}(\alpha,X_2,X_3)=X_2^{i_2-|S_2'[\alpha]|}(\prod_{\beta'\in S_2'[\alpha]} X_2-\beta')f_\alpha(X_2,X_3)$ by Equations (8) (9), thus $g_{\mathbf{i}}$ vanishes on $\pi_{3,2}^{-1}(S_2'[\alpha])$. It follows that $g_{\mathbf{i}}$ vanishes on $\{X_1=\alpha\}\cap V^{>i_3}$, hence on $V^{>i_3}\cap V^{i_3,\leq i_2}$, (†). For $\beta\in S_2[\alpha]$, $\widetilde{g_{\mathbf{i}}}(\beta,X_3)=\ \mathrm{C}\ f_\alpha(\beta_2,X_3)$ where $\mathrm{C}\ \in\bar{k}$, which by Equation (9) vanishes on $V[\beta]$. Hence, $g_{\mathbf{i}}$ vanishes on $V\cap\pi_{3,2}^{-1}(S_2)\cap\pi_{3,1}^{-1}(S_1)=V^{\leq i_3}\cap V^{i_3,\leq i_2}$. With (†), $g_{\mathbf{i}}$ vanishes on

$$(V^{\leq i_3}\cap V^{i_3,\leq i_2})\cup(V^{>i_3}\cap V^{i_3,\leq i_2})=(V^{\leq i_3}\cup V^{>i_3})\cap V^{i_3,\leq i_2}=V\cap V^{i_3,\leq i_2}=V^{i_3,\leq i_2}.$$

2.4. Concluding proof

Looking at Equation (4) and Equation (8), let

$$G:=\{g_{\mathbf{i}}\ \mid\ \mathbf{i}\in\mathcal{L}(\widetilde{V})\}.$$

Let also $\mathcal{G}_2$ be a minimal Gröbner basis of $I_2:=I\cap k[X_2,X_2]$. Lemma 3 shows that $G\cup\mathcal{G}_2\subset I$. In this subsection, we show that $G\cup\mathcal{G}_2$ is a minimal Gröbner basis of I. It is sufficient to prove that $\langle\textsc{lm}(I)\rangle=\langle\textsc{lm}(G\cup\mathcal{G}_2)\rangle$, or with the notation of Definition 1, that $\min(I)=\min(G)\cup\min(\mathcal{G}_2)$. This is done by induction on $|G|=|\mathcal{L}(\widetilde{V})|$.

Lemma 4. *Assume that $|G|=1$. Then $\min(I)=\min(\langle G\rangle)\cup\min(\langle\mathcal{G}_2\rangle)$.*

Proof. The proof for the general case $n>3$ is no more complicated than the case $n=3$, it suffices essentially to replace n by 3 in the proof of Lemma 12.

With the base case treated, the induction can be carried through to prove that:

Theorem 1. *In general, the equality $\min(\langle G\cup\mathcal{G}_2\rangle)=\min(I)$ also holds.*

The proof occupies the remaining of the section. It goes by induction on $|G| = |\mathcal{L}(\widetilde{V})|$. The previous lemma treats the base case $|G| = 1$. Assume that $|G| > 1$, and let $\mathbf{i} := \min_{\preccurlyeq} \mathcal{L}(\widetilde{V})$. Define $f := \mathrm{LC}_2(g_{\mathbf{i}})$. Note that $f \neq 1$. Since $\mathbf{i} = (i_2, i_3) \in \mathcal{L}(\widetilde{V})$, then $W := \widetilde{V}^{i_3,i_2}$ is not empty, and since $|G| > 1$, neither is $W' = V \setminus W$. Let $J := I(W)$ and $J' = I(W'$.

We summarize hereunder the next steps heading to the proof of Theorem 1.

1. $\min(I) = \min(J') \setminus \{\mathrm{LM}(f)\} \cup \{\mathrm{LM}(f)m \mid m \in \min(J)\}$.
2. The same equality holds for the X_3-elimination ideals I_2, J_2, J_2' which denotes the intersection with $k[X_1, X_2]$. $\min(I_2) = \min(J_2') \setminus \{\mathrm{LM}(f)\} \cup \{\mathrm{LM}(f)m \mid m \in \min(J_2)\}$
3. By construction $\mathcal{L}(\widetilde{W'}) = \mathcal{L}(\widetilde{V}) \setminus \{(i_2, \ldots, i_n)\}$ therefore the induction hypothesis supplies the equality: $\min(J') = \{X_1^{j_1} X_2^{j_2} X_3^{j_3} \mid (j_1, j_2, j_3) \in \mathcal{L}'(\widetilde{W'})\} \cup \min(J'_{n-1})$.
4. The set W verifies by construction $\mathcal{L}(\widetilde{W}) = \{(i_2, i_3)\}$ hence falls into the case of Lemma 4 which gives: $\min(J) = \{X_3^{i_3}\} \cup \min(J_{n-2}\}$.
5. Putting this in the equality 1. shows that: $\min(I) = \{X_1^{j_1} X_2^{j_2} X_3^{j_3} \mid (j_1, j_2, j_3) \in \mathcal{L}'(\widetilde{W'})\} \cup \min(J'_{n-1}) \setminus \{\mathrm{LM}(f)\} \cup \{X_3^{i_3}\mathrm{LM}(f)\} \cup \{\mathrm{LM}(f)m \mid m \in \min(J_{n-2})\}$.
6. and using the equalities in 2. and $\mathrm{LM}(f) = X_1^{i_1} X_2^{i_2}$ yeilds the equality: $\min(I) = \{X_1^{j_1} X_2^{j_2} X_3^{j_3} \mid (j_1, j_2, j_3) \in \mathcal{L}(\widetilde{V})\} \cup \min(I_2)$. This is equivalent to the statement of Theorem 1.

In the strategy outlined in points 1.-6. above, only the two ones require a proof. The point 2. can be deduced from the point 1., therefore we focus on proving 1. in the following. This occupies the remaining of this section.

Lemma 5. *Let $J := I(W)$ and $J' := I(W')$. These ideals satisfy the equalities $J' = I + \langle f \rangle$, and $J = I : \langle f \rangle$.*

Consequently, letting $J_2' := J' \cap k[X_1, X_2]$ and $J_2 := J \cap k[X_1, X_2]$, also hold $J_2' = I_2 + \langle f \rangle$ and $J_2 = I_2 : \langle f \rangle$.

Proof. All ideals are radical here and thanks to the separability assumptions (H), the Nullstellensatz is satisfied. It suffices thus to prove that $W = V \setminus (V \cap V(f))$ and that $W' = V \cap V(f)$.

To start with, the fact that (i_2, i_3) is minimal in $\mathcal{L}(V)$ implies that $V^{\leq i_3} = V^{i_3}$ and $V^{i_3, \leq i_2} = V^{i_3, i_2}$. In the course of lemma 3, it was shown that given $\alpha_1' \in S_1'$, $f(\alpha_1', X_2) = 0$ thereby $\pi_{31}^{-1}(S_1') \cap V = \pi_{31}^{-1}(\pi_1(V^{i_3, >i_2})) \cap V = V^{i_3, >i_2} \subset V(f)$. And moreover that for $\alpha_1 \in S_1$ and $(\alpha_1, \alpha_2') \in S_2'[\alpha_1]$ $f(\alpha_1, \alpha_2') = 0$, implying that $\pi_{32}^{-1}(S_2' \cap \pi_{21}^{-1}(S_1)) = V^{>i_3} \cap V^{i_3, i_2} \subset V(f)$. Thus, f vanishes on $(V^{>i_3} \cap V^{i_3,i_2}) \cup V^{i_3,>i_2} = V^{>i_3} \cap (V^{i_3,i_2} \cup V^{i_3,>i_2}) \cup V^{i_3,>i_2} = (V^{>i_3} \cap V^{i_3}) \cup V^{i_3,>i_2}$. By construction, $V^{>i_3}$ and V^{i_3} are disjoint, thus f vanishes on $V^{i_3,>i_2}$ yielding $V \setminus V^{i_3,i_2} \subset V(f)$, according to $V = V^{i_3,i_2} \cap V^{i_3,>i_2}$.

Reciprocally, given $(\alpha_1, \alpha_2) \in V^{i_3,i_2}$, the proof of Lemma 3 shows that $f(\alpha_1, alpha_2) \neq 0$, yielding $V \cap V(f) = \emptyset$. It follows that $W' = V \setminus W = V \cap V(f)$, and hence that $W = V \setminus (V \cap V(f))$.

The proof for the ideals in $k[X_1, X_2]$ is similar.

The ideals J and J' are thereby co-maximal in $k[X_1, X_2, X_3]$, as are the ideals J_2 and J_2' in $k[X_1, X_2]$. The following canonical map below is thus an isomorphism

$$\begin{array}{rcl} \phi : k[X_1, X_2, X_3]/I & \longrightarrow & k[X_1, X_2, X_3]/J' \times k[X_1, X_2, X_3]/J \\ p \bmod I & \longmapsto & p \bmod J' \quad , \quad p \bmod J \end{array} \tag{11}$$

Taking leading monomials defines an isomorphism of k-vector spaces, described below on the monomial bases:

$$\begin{array}{rcl} \psi : k[X_1, X_2, X_3]/\langle \mathrm{LM}(I) \rangle & \longrightarrow & k[X_1, X_2, X_3]/\langle \mathrm{LM}(J') \rangle \times k[X_1, X_2, X_3]/\langle \mathrm{LM}(J) \rangle \\ m \bmod \langle \mathrm{LM}(I) \rangle & \longmapsto & m \bmod \langle \mathrm{LM}(J') \rangle \quad , \quad m \bmod \langle \mathrm{LM}(J) \rangle \end{array} \tag{12}$$

In the same way, thanks to Lemma 5 the following isomorphism holds:

$$\begin{array}{rcl} \psi : k[X_1,X_2]/\langle \mathrm{LM}(I_2)\rangle & \longrightarrow & k[X_1,X_2]/\langle \mathrm{LM}(J_2')\rangle \times k[X_1,X_2]/\langle \mathrm{LM}(J_2)\rangle \\ m \bmod \langle \mathrm{LM}(I_2)\rangle & \longmapsto & m \bmod \langle \mathrm{LM}(J_2')\rangle \quad , \quad m \bmod \langle \mathrm{LM}(J_2)\rangle \end{array} \tag{13}$$

In order to prove the points 1. and 2. above, we make explicit the maps (12) and (13). To this end, consider $Y' := \pi_2(W')$ and $Y := \pi_2(W)$, so that $J_2' = I(Y')$ and $J_2 = I(Y)$.

Lemma 6. *Y' is the disjoint union of $\pi_2(V^{>i_3})$ and of $\pi_2(\widetilde{V}^{i_3,>i_2})$.*

Proof. The fact that the two right-hand sets are disjoint comes from $\widetilde{V}^{i_3,>i_2} \subset \widetilde{V}^{i_3}$ and that $\widetilde{V}^{i_3} = V^{i_3}$ which is disjoint from $V^{>i_3}$.

An element (x_1,x_2) of $\pi_2(V)$ is in Y' if and only if it is not in $Y = \pi_2(\widetilde{V}^{i_3,i_2})$. Therefore (x_1,x_2) does not verify $|\pi_{32}^{-1}(x_1,x_2) \cap V| = i_3$ or does not verify $|\pi_{21}^{-1}(x_1) \cap \pi_1(V^{>i_3})| = i_2$. Suppose it does not verify the former. Then by minimality of (i_2,i_3) for $\preccurlyeq$, necessarily $(x_1,x_2) \in \pi_2(V^{>i_3})$. If it does, then (x_1,x_2) does not verify the latter, and $(x_1,x_2) \in \pi_2(\widetilde{V}^{i_3,>i_2})$. This shows that any element of Y' is either is one set or another and reciprocally.

Proposition 2. *$\mathrm{LM}(f)$ is in the minimal monomial basis of $\langle \mathrm{LM}(J_2')\rangle$.*

Proof. From the case $n = 2$ in § 2.1, $\mathrm{LM}(f) = X_1^{i_1}X_2^{i_2}$ is a minimal monomial of $\langle \mathrm{LM}(I_2')\rangle$ if and only if $i_1 := |\pi_1(Y'^{>i_2})|$ as well as if $i_2 \neq 0$ the extra condition $(\widetilde{V}^{i_3,i_2} \neq \emptyset \overset{(\star)}{\Rightarrow} Y'^{i_2} \neq \emptyset)$. Let us prove the latter implication first.

Given $(x_1,x_2,x_3) \in \widetilde{V}^{i_3,i_2}$, by equation (3) $|\pi_{21}^{-1}(x_1) \cap S_2'| = i_2$, equivalently $|\pi_{21}^{-1}(x_1) \cap \pi_2(V^{>i_3})| \overset{(\times)}{=} i_2$. Because $\pi_2(V^{>i_3}) \subset Y'$, holds $|\pi_{21}^{-1}(x_1) \cap Y'| \geq i_2$. Suppose the inequality is strict. There is then a $y = (x_1,y_2) \in Y' \setminus \pi_2(V^{>i_3})$, and by Lemma 6 $y \in \pi_2(\widetilde{V}^{i_3,>i_2})$. Thus, $|\pi_{21}^{-1}(x_1) \cap S_2'| > i_2$, in contradiction with equality $(\times)$. Therefore, $|\pi_{21}^{-1}(x_1) \cap Y'| = i_2$, and since $i_2 \neq 0$ it suffices to pick up an element in $\pi_{21}^{-1}(x_1) \cap Y'$ to prove that $Y'^{i_2} \neq \emptyset$, showing $(\star)$. The other necessary condition concerning i_1 is worked out in the following lemma, which henceforth achieves the proof of Proposition 2.

Lemma 7. *$\pi_1(\widetilde{V}^{i_3,>i_2}) = \pi_1(Y'^{>i_2})$, in particular $i_1 := |\pi_1(\widetilde{V}^{i_3,>i_2})| = |\pi_1(Y'^{>i_2})|$.*

Proof. Given $x_1 \in \pi_1(\widetilde{V}^{i_3,>i_2})$, it verifies by definition $|\pi_{21}^{-1}(x_1) \cap \pi_2(V^{>i_3})| > i_2$. Since $\pi_2(V^{>i_3}) \subset Y'$, this implies that $|\pi_{21}^{-1}(x_1) \cap Y'| > i_2$, equivalently $x_1 \in \pi_1(Y'^{>i_2})$.

Reciprocally, given $y_1 \in \pi_1(Y'^{>i_2})$ it verifies $|\pi_{21}^{-1}(y_1) \cap Y'| \overset{(\cdot)}{>} i_2$. Suppose there is a y_2 such that $(y_1,y_2) \in \pi_2(V^{i_3}) \cap Y'$. Then $(y_1,y_2) \notin \pi_2(\widetilde{V}^{>i_3})$ and thus by Lemma 6 $(y_1,y_2) \in \pi_2(\widetilde{V}^{i_3,>i_2})$ as wanted. If there is no such y_2, then $\pi_{21}^{-1}(y_1) \cap Y' = \pi_{21}^{-1}(y_1) \cap \pi_2(V^{>i_3})$. The inequality $(\cdot)$ gives $|\pi_{21}^{-1}(y_1) \cap \pi_2(V^{>i_3})| > i_2$, which by definition means $y_1 \in \pi_1(\widetilde{V}^{i_3,>i_2})$.

Proposition 2 allows to prove the following:

Lemma 8. *Let $K := \langle \mathrm{LM}(I)\rangle : \langle \mathrm{LM}(f)\rangle$ and $L := \langle \mathrm{LM}(I)\rangle + \langle \mathrm{LM}(f)\rangle$. One has: $K = \langle \mathrm{LM}(J)\rangle$ and $L := \langle \mathrm{LM}(J')\rangle$.*

The same equalities remain true when taking X_3-elimination ideals: if K_2 denotes $K \cap k[X_1,X_2]$ and L_2 denotes $L \cap k[X_1,X_2]$, then hold $K_2 = \langle \mathrm{LM}(J_2)\rangle$ and $L_2 := \langle \mathrm{LM}(J_2')\rangle$.

PROOF. Treating appart the special case $n = 3$ does bring any simplification in regard to the general proof of Corollaries 5 and 6. It almost suffices indeed to replace n by 3. These proofs show as a byproduct that the following isomorpshism of k-vector spaces

$$\begin{array}{rcl} \theta : k[X_1, X_2, X_3]/\langle \mathrm{LM}(I)\rangle & \longrightarrow & k[X_1, X_2, X_3]/L \times k[X_1, X_2, X_3]/K \\ m \bmod \langle \mathrm{LM}(I)\rangle & \longmapsto & m \bmod \mathrm{LM}(f)\ ,\ m \text{ quo } \mathrm{LM}(f) \end{array} \tag{14}$$

coincide with ψ in (12).

The above map (14) proves that $\min(I) = \min(L) \cup \{m\mathrm{LM}(f) \mid m \in \min(K)\}$, and Lemma (8) that $\min(L) = \min(J)$, $\min(K) = \min(J')$, $\min(J_{n-2}) = \min(L_{n-2})$ and $\min(K_{n-2}) = \min(J'_{n-2})$. Thus, $min(I) = \min(J') \cup \{m\mathrm{LM}(f) \mid m \in \min(J)\}$ which is the point 1.

Moreover, the isomorphism θ in (32) allows to deduce without efforts the following one:

$$\begin{array}{rcl} \theta : k[X_1, X_2]/\langle \mathrm{LM}(I_2)\rangle & \longrightarrow & k[X_1, X_2]/L_2 \times k[X_1, X_2]/K_2 \\ m \bmod \langle \mathrm{LM}(I_2)\rangle & \longmapsto & m \bmod \mathrm{LM}(f)\ ,\ m \text{ quo } \mathrm{LM}(f) \end{array}$$

Allowing to prove that $\min(I_{n-2}) = \min(L_2) \setminus \{\mathrm{LM}(f)\} \cup \{\mathrm{LM}(f)m \mid m \in \min(K_2)\}$ and with Lemma 8 that $\min(I_{n-2}) = \min(J'_2) \setminus \{\mathrm{LM}(f)\} \cup \{\mathrm{LM}(f)m \mid m \in \min(J_2)\}$. This is the point 2. aforementioned, and according to the points 1.-6. this achieves the proof of Theorem 1.

3. Combinatorial decomposition of a set of points

The generalization to $n > 3$ coordinates of the decomposition sketched in 2.2 is carried over in this section. Let $V \subset \overline{k}^n$ be the set of common zeroes of the polynomials in I.

3.1. Definitions

There is actually not one decomposition, but one associated to each multi-integer $\mathbf{i} = (i_2, \ldots, i_n) \in \mathbb{N}^{n-1}$, which we **fix** from now on and within this section. The inductive definition requires some notations.

Given S a finite subset of $\overline{k}^\ell$ define:

$$\begin{array}{rcl} \phi_{S,\ell} : V & \longrightarrow & \mathbb{N} \\ y & \longmapsto & |\pi_{\ell,\ell-1}^{-1}(\pi_{\ell-1}(y)) \cap S|. \end{array}$$

This permits to define for each $\ell \in \mathbb{N}$,

$$\widetilde{V}^\ell = V^\ell := \phi_{V,n}^{-1}(\ell)$$

Since V is finite almost all V^ℓ are empty and the family $(V^\ell)_{\ell\in\mathbb{N}}$ is a partition of V. Let i_n be the last coordinate of $\mathbf{i}$ and introduce the following notations:

$$V^{>i_n} := \bigcup_{\ell > i_n} V^\ell \quad \text{and} \quad V^{\leq i_n} := \bigcup_{\ell \leq i_n} V^\ell, \quad \text{so that} \quad V = V^{\leq i_n} \cup V^{>i_n}.$$

Furthermore, let $S_{n-1} := \pi_{n-1}(V^{\leq i_n})$ and $S'_{n-1} := \pi_{n-1}(V^{>i_n})$.

Consider next i_{n-1} the next to last coordinate of $\mathbf{i}$. Define:

$$V^{i_n,\ell} := \phi^{-1}_{S_{n-1},n-1}(\ell) \qquad \text{and} \qquad \widetilde{V}^{i_n,\ell} := \phi^{-1}_{S_{n-1},n-1}(\ell) \cap \widetilde{V}^{i_n} = V^{i_n,\ell} \cap V^{i_n}. \tag{15}$$

As before, almost all $V^{i_n,\ell}$ are empty, and $(V^{i_n,\ell})_{\ell\in\mathbb{N}}$ is a partition of V. Similarly almost all $\widetilde{V}^{\ell,i_3}$ are empty and those who are not form a partition of $\widetilde{V}^\ell = V^\ell$. Let

$$V^{i_n,\leq i_{n-1}} := \bigcup_{\ell \leq i_{n-1}} V^{i_n,\ell} \quad \text{and} \quad V^{i_n,>i_{n-1}} := \bigcup_{\ell > i_{n-1}} V^{i_n,\ell},$$

and $S_{n-2} := \pi_{n-2}(V^{i_n,\leq i_{n-1}})$, $S'_{n-2} := \pi_{n-2}(V^{i_n,>i_{n-1}})$.

3.2. Induction

Assume that by induction are constructed two families $(S_{n-1},\dots,S_j)$ and $(S_{n-1},\dots,S_j)$, as well as two families:

$$((V^\ell)_{\ell\in\mathbb{N}},(V^{i_n,\ell})_{\ell\in\mathbb{N}},\dots,(V^{i_n,i_{n-1},\dots,i_{j+2},\ell})_{\ell\in\mathbb{N}}),\quad \text{all are partitions of } V$$

and $((V^\ell)_{\ell\in\mathbb{N}},(\widetilde{V}^{i_n,\ell})_{\ell\in\mathbb{N}},\dots,(\widetilde{V}^{i_n,i_{n-1},\dots,i_{j+2},\ell})_{\ell\in\mathbb{N}})$, where $(\widetilde{V}^{i_n,i_{n-1},\dots,i_{j+k},\ell})_{\ell\in\mathbb{N}}$ is a partition of $\widetilde{V}^{i_n,i_{n-1},\dots,i_{j+k}}$, such that $S'_j=\pi_j(V^{i_n,\dots,i_{j+2},>i_{j+1}})$ and $S_j=\pi_j(V^{i_n,\dots,i_{j+2},\le i_{j+1}})$.

Let $\mathbf{k}:=i_n,i_{n-1},\dots,i_j$. The aim now is to construct S_{j-1}, S'_{j-1}, a partition $(V^{\mathbf{k},\ell})_{\ell\in\mathbb{N}}$ of V, and a partition $(\widetilde{V}^{\mathbf{k},\ell})_{\ell\in\mathbb{N}}$ of $\widetilde{V}^{\mathbf{k}}$. Recall that i_j is the j-th coordinate of $\mathbf{k}$.

$$V^{\mathbf{k},\ell}:=\phi^{-1}_{S_j,j}(\ell)\qquad\text{and}\qquad \widetilde{V}^{\mathbf{k},\ell}:=\phi^{-1}_{S_j,j}(\ell)\cap\widetilde{V}^{\mathbf{k}}. \tag{16}$$

Again, the family $(V^{\mathbf{j},\ell})_{\ell\in\mathbb{N}}$ is a partition of V. In a similar way as before, we introduce the following convenient notations:

$$V^{\mathbf{k},\le i_j}:=\bigcup_{\ell\le i_j}V^{\mathbf{k},\ell}\quad\text{and}\quad V^{\mathbf{k},>i_j}:=\bigcup_{\ell>i_j}V^{\mathbf{k},\ell}. \tag{17}$$

Finally, we define $S'_{j-1}:=\pi_{j-1}(V^{\mathbf{k},>i_j})$ and $S'_{j-1}:=\pi_{j-1}(V^{\mathbf{k},\le i_j})$. Despite these two sets depend on V and $\mathbf{i}$, the notations do not refer to this. It will not be confusing though, since the construction above will always be applied to V and $\mathbf{i}$, except in Proposition 3, which forces to precise things and to make the notations heavier in the course of its proof. This achieves the construction of the four families that we sought for.

Using this inductive construction, it is possible to ultimately define the combinatorial decomposition of V that was mentioned in the introduction and in § 2:

$$V=\bigcup_{\ell\in\mathbb{N}}V^{i_n,\dots,i_3,\ell}. \tag{18}$$

The 3 other by-product objects coming with it, $(S_j)_{j=n-1,\dots,1}$, $(S'_j)_{j=n-1,\dots,1}$, and $(\widetilde{V}^{i_n,\dots,i_3,\ell})_{\ell\in\mathbb{N}}$ will reveal also crucial for the interpolation formulas of the next section. Some basic properties related to these objects are also in order.

Lemma 9. *The sets constructed in the § 3.2 above verify the following properties:*

1. $S_j\cap S'_j=\emptyset$ *and* $\pi_j(V)=S_j\cup S'_j$, *for* $1\le j\le n-1$.
2. $\widetilde{V}^{i_n,\dots,i_{\ell+1}}=\{x\in V\mid|\pi^{-1}_{k,k-1}(x_1,\dots,x_{k-1})\cap S'_k|=i_k,\ \ \text{for } k=\ell+1,\dots,n\}$
3. $\pi_\ell(\widetilde{V}^{i_n,\dots,i_{\ell+1}})=\pi_\ell(V^{i_n,\dots,i_{\ell+1}})$, *and therefore* $S'_\ell=\pi_\ell(\widetilde{V}^{i_n,\dots,>i_{\ell+1}})$.

Proof. For Point 1., the first equality is a consequence of: an element $x=(x_1,\dots,x_j)\in S'_j=\pi_j(V^{i_n,\dots,i_{j+2},>i_{j+1}})$ verifies $|\pi^{-1}_{j+1,j}(x)\cap S'_{j+1}|>i_{j+1}$ whereas an element $y=(y_1,\dots,y_j)\in S_j=\pi_j(V^{i_n,\dots,i_{j+2},\le i_{j+1}})$ verifies the condition $|\pi^{-1}_{j+1,j}(x)\cap S'_{j+1}|\le i_{j+1}$, according to Definitions (17) and (16). The second equality is due to the fact that $V^{i_n,\dots,i_{j+2},\le i_{j+1}}\cup V^{i_n,\dots,i_{j+2},>i_{j+1}}=V$ is a partition of V.

Point 2. is a mere restatement of the definitions. Indeed,

$$\widetilde{V}^{i_n,\dots,i_{\ell+1}}=\{x\in\widetilde{V}^{i_n,\dots,i_{\ell+2}}\mid|\pi^{-1}_{\ell+1,\ell}(x_1,\dots,x_\ell)\cap S'_{\ell+1}|=i_{\ell+1}\}.$$

Thus, since $x\in\widetilde{V}^{i_n,\dots,i_{\ell+2}}$ it verifies $|\pi^{-1}_{\ell+2,\ell+1}(x_1,\dots,x_{\ell+1})\cap S_{\ell+1}|=i_{\ell+1}$ as well as $x\in\widetilde{V}^{i_n,\dots,i_{\ell+3}}$ which in turn implies that it verifies $|\pi^{-1}_{\ell+3,\ell+2}(x_1,\dots,x_{\ell+2})\cap S'_{\ell+2}|=i_{\ell+2}$ and so on.

To prove 3. we proceed by decreasing induction on $\ell = n-1, \cdots, 1$. For the base case $\ell = n-1$, we have $\widetilde{V}^{i_n} = V^{i_n}$ and thus $\pi_{n-1}(\widetilde{V}^{i_n}) = \pi_{n-1}(V^{i_n})$. Suppose next that $\pi_j(\widetilde{V}^{i_n,\dots,i_{j+1}}) = \pi_j(V^{i_n,\dots,i_{j+1}})$, for all $j = n-1,\dots,\ell+1$. Given $x \in V^{i_n,\dots,i_{\ell+1}}$, it verifies by definition $|\pi_{\ell+1,\ell}^{-1}(x_1,\dots,x_\ell) \cap S_{\ell+1}| \overset{(o)}{=} i_{\ell+1}$. By induction hypothesis, $(x_1,\dots,x_{\ell+1}) \in \pi_{\ell+1}(\widetilde{V}^{i_n,\dots,i_{\ell+2}})$ and by Point 2. above, verifies $|\pi_{j+1,j}^{-1}(x_1,\dots,j) \cap S'_j| = i_j$ for $j = \ell+2,\dots,n-1$. With the equality (o) and by Point 2., this means that $(x_1,\dots,x_\ell) \in \widetilde{V}^{i_n,\dots,i_{\ell+1}}$. Therefore $\pi_\ell(V^{i_n,\dots,i_{\ell+1}}) \subset \pi_\ell(\widetilde{V}^{i_n,\dots,i_{\ell+1}})$. The other inclusion being clear, this achieves the proof by induction.

The next subsection studies properties of these sets after deletion of one these blocks. This part is crucial for the inductive nature of the proof coming afterward.

3.3. Properties after deletion of the smallest block

As sketched for the case $n = 3$, the multi-integers $\mathbf{i} = (i_2,\dots,i_n)$ for which $\widetilde{V}^{i_n,\dots,i_2}$ is not empty are related to the exponent of the minimal monomial basis. This motivates the generalization of the sets $\mathcal{L}(\widetilde{V})$ and $\mathcal{L}'(\widetilde{V})$ defined in Equation (4) and (5).

Definition 2. *Let $\mathcal{L}(\widetilde{V})$ be the set of $\mathbf{i} = (i_2,\dots,i_n) \in \mathbb{N}^{n-1}$ such that $\widetilde{V}^{i_n,\dots,i_2} \neq \emptyset$. Define:*

$$\mathcal{L}'(\widetilde{V}) := \{(i_1,i_2,\dots,i_n) \in \mathbb{N}^n \mid \ (i_2,\dots,i_n) \in \mathcal{L}(\widetilde{V}) \text{ and } i_1 = |\pi_1(V^{i_n,\dots,i_3,>i_2})|\}.$$

In the remainder of this subsection, is assumed that $|\mathcal{L}'(\widetilde{V})| > 1$, and we let $\mathbf{i} := \min_{\preccurlyeq} \mathcal{L}'(\widetilde{V})$. Let $W := \widetilde{V}^{i_n,\dots,i_2}$, $W' := V \setminus W$ and $Y' := \pi_{n-1}(W')$.

Lemma 10. *Y' is the disjoint union of: $Y' = \pi_{n-1}(\widetilde{V}^{>i_n}) \bigcup_{\ell=2}^{n-1} \pi_{n-1}(\widetilde{V}^{i_n,\dots,>i_\ell})$.*

Proof. From Lemma 9 2., $x \in V^{i_2,\dots,i_n}$ is equivalent to $|\pi_{j+1,j}^{-1}(x_1,\dots,x_j) \cap \pi_j(\widetilde{V}^{i_n,\dots,>i_{j+1}})| \overset{*_j}{=} i_j$ for $j = 2,\dots,n-1$ and $|\pi_{n,n-1}^{-1}(x_1,\dots,x_{n-1}) \cap V| \overset{*_n}{=} i_n$.

Now, $y \in W'$ if and only if $y \notin V^{\mathbf{i}}$ and therefore if and only if there exists a maximal $2 \leq j \leq n$ such that the equality $*_j$ is not true. Then instead of an equality, it can only be a $>$, otherwise $\mathbf{i}$ would not be minimal for $\preccurlyeq$ in $\mathcal{L}'(\widetilde{V})$. From the definitions, it means that $y \in \widetilde{V}^{i_n,\dots,>i_{j+1}}$ and that $y \notin \widetilde{V}^{i_n,\dots,>i_k}$ for $k > j+1$. Neither holds $y \in \widetilde{V}^{i_n,\dots,>i_k}$ for $k < j$ because $\widetilde{V}^{i_n,\dots,>i_k} \subset \widetilde{V}^{i_n,\dots,i_{k+1}} \subset \widetilde{V}^{i_n\dots,i_j}$ for these values of k. This proves that $W' = \widetilde{V}^{>i_n} \bigcup_{\ell=2}^{n-1} \widetilde{V}^{i_n,\dots,>i_\ell}$ and that the union is disjoint. Taking projections π_{n-1} proves the equality in the lemma.

Proposition 3. *We can apply the construction of § 3 to $Y' := \pi_{n-1}(V \setminus \widetilde{V}^{i_n,\dots,i_2})$ and to the multi-integer $\mathbf{j} = (i_2,\dots,i_{n-1})$ instead of V and of $\mathbf{i} = (i_2,\dots,i_n)$. This defines similarly families of sets $Y^{i_{n-1},\dots,i_\ell}$. They verify:*

1. $\pi_\ell(\widetilde{V}^{i_n,\dots,>i_{\ell+1}}) \subset \pi_\ell(Y'^{i_{n-1},\dots,>i_{\ell+1}})$ *for* $\ell = 1,\dots,n-2$.
2. $\widetilde{Y}'^{i_{n-1},\dots,i_2} \neq \emptyset$ *if* $i_{n-1} \neq 0$.
3. $\pi_1(\widetilde{V}^{i_n,\dots,>i_2}) = \pi_1(\widetilde{Y}'^{i_{n-1},\dots,>i_2})$.

Remark: Locally in this proof, we overload the notations S'_ℓ introduced in § 3. Indeed, therein it is attached to V and $\mathbf{i}$, and the notations should refer to them so that no confusion arise with the similar construction attached to Y' and $\mathbf{j}$. Therefore, let $S_\ell'^{V,\mathbf{i}} = \pi_\ell(\widetilde{V}^{i_n,\dots,>i_{\ell+1}})$ and $S_\ell'^{Y',\mathbf{j}} = \pi_\ell(\widetilde{Y}^{i_{n-1},\dots,>i_{\ell+1}})$. With this, Point 1. and Point 3 can be rewritten as:

1. $S_\ell'^{V,\mathbf{i}} \subset S_\ell'^{Y',\mathbf{j}}$ for $\ell = 1, \ldots, n-2$.
3. $S_1'^{V,\mathbf{i}} = S_1'^{Y',\mathbf{j}}$.

PROOF. The first point is proved by decreasing induction on $\ell = n-1, \ldots, 1$. The base step amounts to show that $\pi_{n-1}(V^{>i_n}) \subset Y'$. This is contained in Lemma 10. Next we assume the statement true for a given $\ell + 1 > 1$ and let us prove it for ℓ. Let $x \in \widetilde{V}^{i_n,\ldots,>i_{\ell+1}}$, so that $(x_1, \ldots, x_\ell) \in S_\ell'^{V,\mathbf{i}}$. By definition of $S_\ell'^{V,\mathbf{i}}$, the inequality $|\pi_{\ell+1,\ell}^{-1}(x_1, \ldots, x_\ell) \cap S_{\ell+1}'^{V,\mathbf{i}}| > i_{\ell+1}$ holds. By induction hypothesis, $S_{\ell+1}'^{V,\mathbf{i}} \subset S_{\ell+1}'^{Y',\mathbf{j}}$ hence $|\pi_{\ell+1,\ell}^{-1}(x_1, \ldots, x_\ell) \cap S_{\ell+1}'^{Y',\mathbf{j}}| > i_{\ell+1}$. Consequently, $\phi_{S_{\ell+1}'^{Y',\mathbf{j}},\ell+1}(x) > i_{\ell+1}$ and in virtue of Equality (15), $(x_1, \ldots, x_\ell) \in \pi_\ell(\widetilde{Y}^{i_{n-1},\ldots,>i_{\ell+1}})$.

Let us turn out to the proof of 2. Remember that $\mathbf{i}$ has been chosen as the minimal element of $\mathcal{L}'(V)$ and according to Definition 2, $\widetilde{V}^{\mathbf{i}} \neq \emptyset$. Let $x \in \widetilde{V}^{\mathbf{i}}$ fixed. For $\ell = 2, \ldots, n-1$ define $A_\ell := \pi_{\ell,\ell-1}^{-1}(x_1, \ldots, x_{\ell-1}) \cap S_\ell'^{V,\mathbf{i}}$ and $A_n := \pi_{n,n-1}^{-1}(x_1, \ldots, x_n) \cap V$. By Lemma 9 point 2., $x \in \widetilde{V}^{\mathbf{i}}$ is equivalent to $|A_\ell| = i_\ell$ for $\ell = 2, \ldots, n$. Let us prove that for $\ell = 1, \ldots, n-1$ holds $|B_\ell| = i_\ell$, where $B_\ell := \pi_{\ell,\ell-1}^{-1}(x_1, \ldots, x_{\ell-1}) \cap \pi_\ell(\widetilde{Y'}^{i_{n-1},\ldots,>i_{\ell+1}})$ if $\ell < n-1$ (and $B_{n-1} := \pi_{n-1,n-2}^{-1}(x_1, \ldots, x_{n-2}) \cap Y'$). According to Point 1., $S_\ell'^{V,\mathbf{i}} \subset S_\ell'^{Y',\mathbf{j}}$ yielding $|A_\ell| \leq |B_\ell|$. We show that for each ℓ a strict inequality $|A_\ell| < |B_\ell|$ can not occur.

Assume first $\ell = n-1$. If the inequality $|A_\ell| \leq |B_\ell|$ were strict, then there would exist $y = (x_1, \ldots, x_{n-2}, y_{n-1}) \in Y' \setminus S_{n-1}'^{V,\mathbf{i}}$. By Lemma 10 $y \in \pi_{n-1}(\widetilde{V}^{i_n,\ldots,>i_k})$ for a $2 \leq k \leq n-1$, Then $|\pi_{k,k-1}^{-1}(x_1, \ldots, x_{k-1}) \cap S_k'^{V,\mathbf{i}}| > i_k$, contradicts $|A_k| = i_k$. Therefore there is no such y, and $|B_{n-1}| = |A_{n-1}| = i_{n-1}$.

Next assume that $\ell < n-1$ and suppose again that the inequality $|A_\ell| \leq |B_\ell|$ is strict. Thus there is a $y = (x_1, \ldots, x_{\ell-1}, y_\ell) \in S_\ell'^{Y',\mathbf{j}} \setminus S_\ell'^{V,\mathbf{i}}$. By Lemma 10, y belongs either to $\pi_\ell(\widetilde{V}^{i_n,\ldots,>i_{k+1}})$ for a $1 \leq k \leq n-2$ distinct from ℓ, either to $\pi_\ell(V^{>i_n})$. Note that $k < \ell$ can not occur since $\pi_k(y) = \pi_k(x) \in \pi_k(V^{\mathbf{i}}) \subset \pi_k(\widetilde{V}^{i_n,\ldots,i_{k+1}}) = S_k^{V,\mathbf{i}}$ would contradict $\pi_k(y) \in \pi_k(\widetilde{V}^{i_n,\ldots,>i_{k+1}}) = S_k'^{V,\mathbf{i}}$, according that $S_k'^{V,\mathbf{i}} \cap S_k^{V,\mathbf{i}} = \emptyset$. Thus $y \in \pi_\ell(\widetilde{V}^{i_n,\ldots,>i_{k+1}})$ for a $k > \ell$. Since $y \notin S_\ell'^{V,\mathbf{i}}$, necessarily $y \in S_\ell^{V,\mathbf{i}}$ by point 1. of Lemma 9 and y verifies: $|\pi_{\ell+1,\ell}^{-1}(y) \cap S_{\ell+1}'^{V,\mathbf{i}}| = i_{\ell+1}$. On the other hand, $y \in S_\ell'^{Y',\mathbf{j}}$ and thus holds $|\pi_{\ell+1,\ell}^{-1}(y) \cap S_{\ell+1}'^{Y',\mathbf{j}}| > i_{\ell+1}$. This means that there is an element $y^{(1)} = (x_1, \ldots, x_{\ell-1}, y_\ell, y_{\ell+1}) \in S_{\ell+1}'^{Y',\mathbf{j}} \setminus S_{\ell+1}'^{V,\mathbf{i}}$. By Lemma 10, $y^{(1)} \in \pi_{\ell+1}(\widetilde{V}^{i_n,\ldots,>i_{k_1+1}})$ for a $1 \leq k_1 \leq n-2$ distinct from $\ell+1$, or $y^{(1)} \in \pi_{\ell+1}(V^{>i_n})$. As shown above $k_1 < \ell$ leads to a contradiction. Similarly, $k_1 = \ell$ is not possible since $\pi_{k_1}(y^{(1)}) = \pi_{k_1}(y) \notin S_{k_1}'^{V,\mathbf{i}}$, and thus $y^{(1)} \notin \pi_{\ell+1}(\widetilde{V}^{i_n,\ldots,>i_{\ell+1}})$. Consequently, $k_1 > \ell+1$. Since $y^{(1)}$ belongs to $S_{\ell+1}^{V,\mathbf{i}}$, one has $|\pi_{\ell+2,\ell+1}^{-1}(y^{(1)}) \cap S_{\ell+2}'^{V,\mathbf{i}}| = i_{\ell+2}$. On the other hand, $y^{(1)} \in S_{\ell+1}'^{Y',\mathbf{j}}$ gives $|\pi_{\ell+2,\ell+1}^{-1}(y^{(1)}) \cap S_{\ell+2}'^{Y',\mathbf{j}}| > i_{\ell+2}$, proving the existence of an element $y^{(2)} \in S_{\ell+2}'^{Y',\mathbf{j}} \setminus S_{\ell+2}'^{V,\mathbf{i}}$. We can repeat similar arguments as used above, leading to the existence of $k_2 > \ell+2$ such that $y^{(2)} \in \pi_{\ell+2}(\widetilde{V}^{i_n,\ldots,>i_{k_2+1}})$. More generally, this repetition gives a sequence $y = y^{(0)}, y^{(1)}, \ldots, y^{(t)}$, with $t = n-1-\ell$, where each $y^{(r)} \in S_{\ell+r}'^{Y',\mathbf{j}} \setminus S_{\ell+r}'^{V,\mathbf{i}}$ for $r < t$, and $y^{(t)} \in Y' \setminus S_{n-1}'^{V,\mathbf{i}}$; as well as $y^{(r)} \in \pi_{\ell+r}(\widetilde{V}^{i_n,\ldots,>i_{k_r+1}})$ for a $k_r > \ell + r$, and moreover $\pi_r(y^{(r+1)}) = y^{(r)}$ for $r < t$. The last possibility is then $y^{(t)} \in Y' \setminus S_{n-1}'^{V,\mathbf{i}}$. By Lemma 10 this implies $y^{(t)} \in \pi_{n-1}(\widetilde{V}^{i_n,\ldots,>i_{k_t+1}})$. As already seen, $k_t > \ell$, so that $\pi_{k_t}(y^{(t)}) = y^{(k_t-\ell)} \in S_{k_t}'^{V,\mathbf{i}}$. This contradicts $y^{(k_t-\ell)} \in S_{k_t}'^{Y',\mathbf{j}} \setminus S_{k_t}'^{V,\mathbf{i}}$. We conclude that the initial assumption $|A_\ell| < |B_\ell|$ does not hold.

Therefore, $|B_\ell| = i_\ell$ for $\ell = 2, \ldots, n-1$ and by Lemma 9 3., it comes $(x_1, \ldots, x_{n-2}) \in \pi_{n-2}(Y'^{\mathbf{j}})$, and moreover $|\pi_{n-1,n-2}^{-1}(x_1, \ldots, x_{n-2}) \cap Y'| = i_{n-1}$. If $i_{n-1} \neq 0$, it suffices to pick up an element in this set to show that $Y'^{i_{n-1},\ldots,i_2} \neq \emptyset$.

As for the point 3., the inclusion $\subset$ is given by the point 1. with $\ell = 1$. To prove the inclusion $\supset$, consider an element $y = (y_1, \ldots, y_{n-1}) \in Y'^{i_{n-1},\ldots,>i_2}$. By Lemma 10, there

is a $1 \leq k \leq n-2$ such that $y \in \pi_{n-1}(\widetilde{V}^{i_n,\dots,>i_{k+1}})$, or $y \in S'^{V,\mathbf{i}}_{n-1}$. If $k=1$, then $y_1 \in \pi_1(\widetilde{V}^{i_n,\dots,>i_2})$ as wanted. Else $2 \leq k \leq n-2$ and $|\pi^{-1}_{k+1,k}(y_1,\dots,y_k) \cap S'^{V,\mathbf{i}}_{k+1}| > i_{k+1}$. By the point 1., $S'^{V,\mathbf{i}}_{k+1} \subset S'^{Y',\mathbf{j}}_{k+1}$ yielding $|\pi^{-1}_{k+1,k}(y_1,\dots,y_k) \cap S'^{Y',\mathbf{j}}_{k+1}| \overset{*_{k+1}}{>} i_{k+1}$ if $k \leq n-3$ and else $|\pi^{-1}_{n-1,n-2}(y_1,\dots,y_{n-2}) \cap Y'| \overset{*_{n-1}}{>} i_{n-1}$. But $y \in \widetilde{Y}'^{i_{n-1},\dots,>i_2} \subset \widetilde{Y}'^{i_{n-1},\dots,i_3}$ and therefore by Lemma 9 2. the equalities $|\pi^{-1}_{k+1,k}(y_1,\dots,y_k) \cap S'^{Y',\mathbf{j}}_{k+1}| = i_{k+1}$ for $k=3,\dots,n-3$, and additionally the equality $|\pi^{-1}_{n-1,n-2}(y_1,\dots,y_{n-2}) \cap Y'| = i_{n-1}$ must be satisfied. This contradicts the strict inequality $*_{k+1}$.

4. Interpolation formula

The goal is to generalize Equation (8) to $n > 3$ variables. Have in mind the notations of the first paragraph of § 2.3.

4.1. Iterated Lagrange interpolation polynomials

Let A be a k-algebra such that $A \cap k[x] = k$, and $f : \overline{k} \to A$. The *Lagrange interpolation polynomial* of f along U is:

$$L_U(f)(x) := \sum_{\alpha \in U} f(\alpha)\ell_\alpha(x) \in A[x]. \tag{19}$$

To fit the needs of this work, a modification of this polynomial is in order: Let $U' \subset \overline{k}$ be such that $U \cap U' = \emptyset$. Then define:

$$L_{(U,U')}(f)(x) := \left(\prod_{\alpha' \in U'} x - \alpha'\right) L_U(f)(x) = \left(\prod_{\alpha' \in U'} x - \alpha'\right)\left\{\sum_{\alpha \in U} \ell_\alpha(x) f(\alpha)\right\}. \tag{20}$$

Iteration. Given two families of t couples of sets $\mathbf{U} := (U_i)_{i=1,\dots,t}$, $\mathbf{U}' := (U'_i)_{i=1,\dots,t}$ verifying $U_i, U'_i \subset \overline{k}^i$ Zariski-closed over k, $U_i \cap U'_i = \emptyset$, define

$$\mathcal{U}_t := \{(\alpha_1,\dots,\alpha_t) \in \overline{k}^t \mid \alpha_1 \in U_1,\ (\alpha_1,\alpha_2) \in U_2,\dots,\ (\alpha_1,\dots,\alpha_t) \in U_t\}. \tag{21}$$

We aim at defining for each function $f_t : \mathcal{U}_t \to A_t$ where $A_t := \overline{k}[X_{t+1},\dots,X_n]$, a polynomial:

$$\begin{array}{rccl} L_{\mathbf{U},\mathbf{U}'}(\,\cdot\,)(X_1,\dots,X_t) : A_t^{\mathcal{U}_t} & \longrightarrow & A_t[X_1,\dots,X_t] \\ f_t & \longmapsto & L_{\mathbf{U},\mathbf{U}'}(f_t)(X_1,\dots,X_t) \end{array}$$

Equality (20) provides the case $t=1$. Else, we proceed by induction.

Let $\alpha \in \mathcal{U}_{t-1}$. We use the coordinate functions p_i and p_{ij} defined in § 2.1. Using Equation (1) define $T_t^\alpha := p_t(U_t[\alpha])$, $T_t'^\alpha := p_t(U'_t[\alpha]) \subset \bar{k}$. Since $U_t \cap U'_t = \emptyset$, is verified $T_t^\alpha \cap T_t'^\alpha = \emptyset$ as well. Let $d_t := \max_{\beta \in \mathcal{U}_{t-1}} |T_t'^\beta|$. Define:

$$\begin{array}{rccl} g : \mathcal{U}_{t-1} & \longrightarrow & A_t[X_t] = A_{t-1} \\ \alpha & \longmapsto & X_t^{d_t - |T_t'^\alpha|} L_{(T_t^\alpha, T_t'^\alpha)}(f_t)(X_t) \end{array} \tag{22}$$

Let $\mathbf{U}_{\leq t-1} := (U_1,\dots,U_{t-1})$ and $\mathbf{U}'_{\leq t-1} := (U'_1,\dots,U'_{t-1})$. Assume defined inductively

$$L_{\mathbf{U}_{\leq t-1},\mathbf{U}'_{\leq t-1}}(f_{t-1})(X_1,\dots,X_{t-1}) \in A_{t-1}[X_1,\dots,X_{t-1}]$$

for any function $f_{t-1} : \mathcal{U}_{t-1} \to A_{t-1}$. Then let:

$$L_{\mathbf{U},\mathbf{U}'}(f_t)(X_1,\dots,X_t) := L_{\mathbf{U}_{\leq t-1},\mathbf{U}'_{\leq t-1}}(g)(X_1,\dots,X_{t-1}). \tag{23}$$

Explicit form. While this definition is simple and convenient, it is quite obscure. It is possible to give an explicit non-recursive formula. Consider to this end the following:

Lemma 11. *Let $1 \leq s < t$ and for each $\alpha \in \mathcal{U}_s$ define the two sequences $\mathbf{T}_s^\alpha = (T_1^\alpha, \ldots, T_{t-s}^\alpha)$ and $\mathbf{T}'^\alpha_s = (T'^\alpha_1, \ldots, T'^\alpha_{t-s})$ as follows;*

$$T_1^\alpha := p_{s+1}(U_{s+1}[\alpha])\ ,\ T_2^\alpha := p_{s+2,s+1}(\pi_{s+2,s}^{-1}(\alpha) \cap U_{s+2})\ ,\ \ldots\ ,\ T_{t-s}^\alpha := p_{t,s+1}(\pi_{t,s+1}^{-1}(\alpha) \cap U_t).$$

(Similarly are defined the T'^α_j, equal to $p_{j,s+1}(\pi_{j,s}^{-1}(\alpha) \cap U'_j) \subset \overline{k}^{j-s}$ for $j \geq s+1$). Let:

$$\begin{array}{rcl} h : \mathcal{U}_s & \to & A_t[X_{s+1}, \ldots, X_t] \\ \alpha & \mapsto & L_{\mathbf{T}_s^\alpha, \mathbf{T}'^\alpha_s}(f_t)(X_{s+1}, \ldots, X_t) \end{array} \tag{24}$$

Then the following equality holds:

$$L_{\mathbf{U},\mathbf{U}'}(f_t)(X_1, \ldots, X_t) = L_{\mathbf{U}_{\leq s}, \mathbf{U}'_{\leq s}}(h)(X_1, \ldots, X_s).$$

Proof. It is easily done by decreasing induction on s starting from $s = t-1$. This latter case is treated in Equation (23).

Corollary 2 (Explicit interpolation formula). *With the notations above, and the new following one*[5]*, $\alpha^i := (\alpha_1^i, \ldots, \alpha_i^i) \in U_i$, $\alpha'^i := (\alpha'^i_1, \ldots, \alpha'^i_i) \in U'_i$, the polynomial $L_{\mathbf{U},\mathbf{U}'}(f_t)(X_1, \ldots, X_t)$ can be written explicitly as follows, generalizing the case of 3 unknowns in* (8)

$$\left(\prod_{\alpha'^1 \in U'_1} X_1 - \alpha'^1_1\right)\left(\sum_{\alpha^1 \in U_1} \ell_{\alpha_1^1}(X_1) X_2^{d_2 - |U'_2[\alpha^1]|} \prod_{\alpha'^2 \in U'_2[\alpha^1]} (X_2 - \alpha'^2_2)\left(\sum_{\alpha^2 \in U_2[\alpha^1]} \ell_{\alpha_2^2}(X_2) X_3^{d_3 - |U'_3[\alpha^2]|}\right.\right.$$
$$\left.\left. \cdots X_t^{d_t - |U'_t[\alpha^{t-1}]|} \prod_{\alpha'^t \in U'_t[\alpha^{t-1}]} (X_t - \alpha'^t_t)\left(\sum_{\alpha^t \in U_t[\alpha^{t-1}]} \ell_{\alpha_t^t}(X_t) f_t(\alpha^t)\right)\cdots\right)\right).$$

Proof. Again, this is easily seen by induction on t, using Lemma 11 or Equation (23).

More in the spirit of interpolation formulas, it is convenient to provide an expanded version of the formula. Let $\mathbf{a} := (\alpha_1, \alpha_2^2, \ldots, \alpha_t^t)$ as in Corollary 2 and define:

$$\mathscr{L}_{\mathbf{a}}(X_1, \ldots, X_n) := \prod_{i=1}^{t} \ell_{\alpha_i^i}(X_i) \tag{25}$$

Thus, given another point[6] $\mathbf{b} = (\beta^1, \beta^2, \ldots, \beta^t)$ such that $\beta^1 \in U_1$ and $\beta^i \in U_i[\beta^{i-1}]$ for $2 \leq i \leq t-1$ comes:

$$\mathscr{L}_{\mathbf{a}}(\beta^1, \beta_2^2, \ldots, \beta_t^t) = \begin{cases} 1 & \text{if } \mathbf{a} = \mathbf{b} \\ 0 & \text{else} \end{cases}.$$

Define the *expanded explicit form* of $L_{\mathbf{U},\mathbf{U}'}(f_t)$ as:

$$L_{\mathbf{U},\mathbf{U}'}(f_t) = \sum_{\alpha^1 \in U_1, \alpha^2 \in U_2[\alpha^1], \ldots, \alpha^t \in U_t[\alpha^{t-1}]} \mathscr{L}_{\mathbf{a}}(X_1, \ldots, X_t)\left(\prod_{i=1}^{t} X_i^{d_i - |U'_i[\alpha^{i-1}]|} \prod_{\alpha' \in U'_i[\alpha^{i-1}]} (X_i - \alpha'_i)\right) f_t(\alpha) \tag{26}$$

Let us investigate a natural property held by these iterated Lagrange interpolation polynomials.

[5] α^i does NOT denote the i-th power of α. This is a mere shorthand notation.

[6] Again, β^t is not a power of β

Corollary 3. *Assume that $f_t : \mathcal{U}_t \to A_t$ verifies $\mathrm{LM}(f_t(\beta)) = m$ for all $\beta \in \mathcal{U}_t$. Then*

$$\mathrm{LM}(L_{\mathbf{U},\mathbf{U}'}(f_t)(X_1,\ldots,X_t)) = X_1^{d_1}\cdots X_t^{d_t} m.$$

PROOF. Assume that $t = 1$. Then $A_1 := \bar{k}[X_2,\ldots,X_n]$, and $L_{\mathbf{U},\mathbf{U}'}(f_1)(X_1)$ is given by Equation (20). From this equation and Equation (7), we deduce that $\mathrm{LM}(\sum_{\gamma\in U_1}\ell_\gamma(X_1)f_1(\gamma)) = m$, and a look at the explicit form of $g_{\mathbf{i}}$ in Corollary 2 shows that $\mathrm{LM}(L_{\mathbf{U},\mathbf{U}'}(f_1)(X_1)) = X_1^{d_1}m$, as expected.

Assume the corollary true for any function $f_i : \mathcal{U}_i \to A_i$, for $i \le t-1$, and verifying $\mathrm{LM}(f_i(\beta)) = m'$, for all $\beta \in \mathcal{U}_i$. Let the function $g : \mathcal{U}_{t-1} \to A_{t-1}$ as defined in Equation (22). For $\alpha \in \mathcal{U}_{t-1}$ holds $g(\alpha) = X_t^{d_t - |T_t'^\alpha|} L_{(T_t^\alpha, T_t'^\alpha)}(f_t)(X_t)$. By definition,

$$L_{(T_t^\alpha,T_t'^\alpha)}(f_t)(X_t) = \left(\prod_{\gamma'\in T_t'^\alpha} X_t - \gamma_t'\right)\left(\sum_{\gamma\in T_t^\alpha}\ell_{\gamma_t}(X_t)f_t(\gamma)\right).$$

and $d_t := \max_{\alpha\in\mathcal{U}_{t-1}}|T_t'^\alpha|$. Now, by Equation (7), $\mathrm{LM}(\sum_{\gamma\in T_t^\alpha}\ell_{\gamma_t}(X_t)f_t(\gamma)) = m$. It follows that

$$\mathrm{LM}(g(\alpha)) = \mathrm{LM}(X_t^{d_t-|T_t'^\alpha|}L_{T_t^\alpha,T_t'^\alpha}(f_t)(X_t)) = X_t^{d_t}m,$$

for all $\alpha \in \mathcal{U}_{t-1}$. The induction hypothesis applied to g in Equation (23) permits to conclude.

4.2. Application to the settings of § 3

Of course, the above construction is tailored to be used with the two sequences $(S_1,\ldots,S_{n-1})$ and $(S_1',\ldots,S_{n-1}')$ of sets introduced in the previous section. Recall that the algebras A_t are equal to $\overline{k}[X_{t+1},\ldots,X_n]$ for $t = 1,\ldots,n-1$.

Definition 3. $\mathbf{i} := (i_2,\ldots,i_n) \in \mathbb{N}^{n-1}$ *be such that for all* $j = n,\ldots,2$, $\widetilde{V}^{i_n,\ldots,i_3,i_2} \neq \emptyset$. *And define* $\mathbf{S} := (S_1,\ldots,S_{n-1})$, $\mathbf{S}' := (S_1',\ldots,S_{n-1}')$ *obtained from the decomposition of* V *and attached to* $\mathbf{i}$ *of § 3. Let*

$$\mathcal{S}_{n-1} := \{(a_1,\ldots,a_{n-1}) \ : \ a_1\in S_1,\ (a_1,a_2)\in S_2,\ldots,\ (a_1,\ldots,a_{n-1})\in S_{n-1}\},$$

and $f_V : \mathcal{S}_{n-1} \to \overline{k}[X_n]$, $\alpha \mapsto X_n^{i_n-|V[\alpha]|}\prod_{\beta\in V[\alpha]}X_n - \beta_n$. *With these notations, define the polynomial:*

$$g_{\mathbf{i}} := L_{\mathbf{S},\mathbf{S}'}(f_V)(X_1,\ldots,X_{n-1}) \in \overline{k}[X_1,\ldots,X_n]$$

As done for the case $n = 3$, these are candidates for a minimal Gröbner basis of I. Before proving this in § 5 let us show that these polynomials verify the conclusions of Theorem (Structure) stated in the introduction.

Corollary 4. *The leading monomial of* $g_{\mathbf{i}}$ *is* $X_1^{i_1}\cdots X_n^{i_n}$.

PROOF. It suffices to show that for any $\alpha \in \mathcal{S}_{n-1}$, $\mathrm{LM}(f_V(\alpha)) = X_n^{i_n}$ and to apply Corollary 3. The former is clear from the definition of f_V.

Next, let us adapt the construction of Lemma 11 to $g_{\mathbf{i}}$. Fix $1 \le t \le n-1$ and take $\alpha \in \mathcal{S}_t$. Define $\mathbf{T}^\alpha = (T_1^\alpha,\ldots,T_{n-t}^\alpha)$ and $\mathbf{T}'^\alpha = (T_1'^\alpha,\ldots,T_{n-t}'^\alpha)$ as below (p_{ij} is defined in the beginning of the § 2.1):

$$T_1^\alpha := p_{t+1}(S_{t+1}[\alpha])\ ,\ T_2^\alpha := p_{t+2,t+1}(\pi_{t+2,t}^{-1}(\alpha)\cap S_{t+2}),\ldots,T_{n-t}^\alpha := p_{n,t+1}(\pi_{n,t+1}^{-1}(\alpha)\cap S_{n-1}).$$

And similarly using S'_j rather than S_j to define T'^{α}_{j+1}. Let $h_t : \mathcal{U}_t \to A_t[X_{t+1}, \ldots, X_n]$, $\alpha \mapsto L_{\mathbf{T}^{\alpha}_t, \mathbf{T}'^{\alpha}_t}(f_V)(X_{t+1}, \ldots, X_n)$. Lemma 11 gives:

$$g_{\mathbf{i}} = L_{\mathbf{S}_{\leq t}, \mathbf{S}'_{\leq t}}(h_t)(X_1, \ldots, X_t) \tag{27}$$

And moreover, the expanded form gives:

$$g_{\mathbf{i}} = \sum_{\alpha^1 \in S_1, \alpha^2 \in S_2[\alpha^1], \ldots, \alpha^t_t \in S_t[\alpha^{t-1}]} \mathscr{L}_{\mathbf{a}}(X_1, \ldots, X_t) \left(\prod_{j=1}^{t} X_j^{i_j - |S_j[\alpha^{j-1}]|} \prod_{\alpha'^j \in S'_j[\alpha^{j-1}]} (X_j - \alpha'^j_j) \right) h_t(\alpha^t). \tag{28}$$

This recursive point of view is useful for the next Proposition:

Proposition 4. *For each t as above, there is a polynomial $C_t \in k[X_1, \ldots, X_t]$ such that for all $\alpha \in \pi_t(V)$, $g_{\mathbf{i}}(\alpha, X_{t+1}, \ldots, X_n) = C_t(\alpha) h_t(\alpha)$.*

Moreover, if $\alpha \in \mathcal{S}_t$ then $C_t(\alpha) \neq 0$ and if $\alpha \in \pi_t(V) \setminus \mathcal{S}_t$ then $C_t(\alpha) = 0$.

Proof. It suffices to take

$$C_t = \sum_{\alpha^1 \in S_1, \alpha^2 \in S_2[\alpha^1], \ldots, \alpha^t_t \in S_t[\alpha^{t-1}]} \mathscr{L}_{\alpha}(X_1, \ldots, X_t) \prod_{j=1}^{t} X_j^{i_j - |S_j[\alpha^{j-1}]|} \left(\prod_{\alpha'^j \in S'_j[\alpha^{j-1}]} X_j - \alpha'^j_j \right).$$

Indeed, using the expanded explicit form of $g_{\mathbf{i}}$ above, Equation (28) implies that:

$$g_{\mathbf{i}}(\alpha, X_{t+1}, \ldots, X_n) = \prod_{j=1}^{t} (\alpha_j)^{i_j - |S'_j[\pi_{j-1}(\alpha)]|} \left(\prod_{\alpha'^j \in S'_j[\pi_{j-1}(\alpha)]} (\alpha_j - \alpha'^j_j) \right) h_t(\alpha).$$

Hence, $C_t(\alpha) = \prod_{j=1}^{t} (\alpha_j)^{i_j - |S'_j[\pi_{j-1}(\alpha)]|} \left(\prod_{\alpha'^j \in S'_j[\pi_{j-1}(\alpha)]} (\alpha_j - \alpha'^j_j) \right)$. If $\alpha \in \mathcal{S}_t$, then by Lemma 9 point 1., it arrives $\prod_{\alpha'^j \in S'_j[\pi_{j-1}(\alpha)]} (\alpha_j - \alpha'^j_j) \neq 0$. And on the contrary, if $\alpha \notin \mathcal{S}_t$, then there exists j such that $(\alpha_1, \ldots, \alpha_j) \in S'_j$, implying that $\prod_{\alpha'^j \in S'_j[\pi_{j-1}(\alpha)]} (\alpha_j - \alpha'^j_j) = 0$ and henceforth $C_t(\alpha) = 0$.

Naturally, the interpolation polynomials $g_{\mathbf{i}}$ verify Theorem (structure) of the introduction.

Proposition 5. *For $1 \leq t \leq n-1$, the polynomial $g_{\mathbf{i}}$ verifies:*

$$g_{\mathbf{i}} \in \langle \mathrm{LC}_1(g_{\mathbf{i}}) \rangle, \quad \textit{and for} \quad 2 \leq t \leq n-1, \quad g_{\mathbf{i}} \in \langle \mathrm{LC}_t(g_{\mathbf{i}}) \rangle + I_{t-1}.$$

Proof. If $t = 1$ then Corollary 2 clearly shows that $\mathrm{LC}_1(g_{\mathbf{i}}) = \prod_{\alpha'_1 \in S'_1} X_1 - \alpha'_1$ divides $g_{\mathbf{i}}$.

Assume $t \geq 2$. Let $\alpha \in \mathcal{S}_{t-1}$. Then Proposition 4 implies that $\mathrm{LC}_t(g_{\mathbf{i}}(\alpha, X_t, \ldots, X_n)) = C_{t-1}(\alpha) \mathrm{LC}_t(h_{t-1}(\alpha))$. On the other hand, define $T^{\alpha} := S_t[\alpha]$ and $T'^{\alpha} := S'_t[\alpha]$. Then by the recursive equality (23), $h_{t-1}(\alpha) = L_{T^{\alpha}, T'^{\alpha}}(h_t(\alpha, X_t))$, so that

$$h_{t-1}(\alpha) = X_t^{i_t - |S_t[\alpha]|} \prod_{\beta' \in T'^{\alpha}} (X_t - \beta'_t) \left(\sum_{\beta \in T^{\alpha}} \ell_{\beta_t}(X_t) h_t(\beta) \right).$$

It follows that $\mathrm{LC}_t(g_{\mathbf{i}}(\alpha, X_t, \ldots, X_n)) = C_{t-1}(\alpha)(X_t^{i_t - |S_t[\alpha]|} \prod_{\beta' \in T'^{\alpha}} (X_t - \beta'_t))$ divides $h_{t-1}(\alpha)$ for all $\alpha \in \mathcal{S}_{t-1}$, and thus divides $g_{\mathbf{i}}(\alpha, X_t, \ldots, X_n)$.

If $\alpha \in \pi_{t-1}(V) \setminus \mathcal{S}_{t-1}$ then Proposition 4 shows that $C_{t-1}(\alpha) = 0$ hence that $\mathrm{LC}_t(g_{\mathbf{i}}(\alpha, X_t, \ldots, X_n)) = g_{\mathbf{i}}(\alpha, X_t, \ldots, X_n) = 0$. Therefore, $g_{\mathbf{i}} - C_{t-1}(\alpha) \mathrm{LC}_t(g_{\mathbf{i}})$ vanishes on $\pi_{t-1}(V)$. This implies that $g_{\mathbf{i}} \in \langle \mathrm{LC}_t(g_{\mathbf{i}}) \rangle + I_{t-1}$.

5. Concluding proof: leading monomial

This last section is devoted to prove that the polynomials $g_{\mathbf{i}}$ of Definition 3 form a minimal Gröbner basis of I. To achieve this, we follow the gist of the strategy of the case $n = 3$ of § 2.4.

Let $G := \{g_{\mathbf{i}} \mid \mathbf{i} \in \mathcal{L}(\widetilde{V})\}$. By induction on the number of variables n, we can suppose that a minimal Gröbner basis $\mathcal{G}_{n-1}$ of I_{n-1} is given by the polynomials constructed in Definition 3. The first step is to show that each polynomial $g_{\mathbf{i}}$ vanishes on V. The second step consists in proving the equality of leading monomial ideals: $\langle \textsc{lm}(I)\rangle = \langle \textsc{lm}(\langle G \cup \mathcal{G}_{n-1}\rangle)\rangle$.

Theorem 2. *Each polynomial $g_{\mathbf{i}} \in G$ vanishes on V.*

Proof. Let $\beta \in V$ and $\alpha := \pi_{n-1}(V)$. The analysis done for the proof of Proposition 5 shows that if $\alpha \notin \mathcal{U}_{n-1}$ then $g_{\mathbf{i}}(\alpha, X_n) = 0$, henceforth $g_{\mathbf{i}}(\beta) = 0$ as well. Suppose that $\alpha \in \mathcal{U}_{n-1}$. By Proposition 4 $g_{\mathbf{i}}(\alpha, X_n) \overset{(*)}{=} C_{n-1}(\alpha) h_{n-1}(\alpha)$, where $h_{n-1} = f_V$ (see definition of the function f_V in Definition 3). In particular $h_{n-1}(\alpha) = X_n^{i_n - |V[\alpha]|} \prod_{\gamma \in V[\alpha]} X_n - \gamma_n$. Now β being in $V[\alpha]$, it comes $h_{n-1}(\alpha) = 0$, implying by $(*)$ that $g_{\mathbf{i}}(\beta) = 0$.

Lemma 12. *If $|G| = 1$ then $\min(I) = \min(\langle G\rangle) \cup \min(\langle \mathcal{G}_{n-1}\rangle)$.*

Proof. If $|G| = 1$, then only one V^ℓ is not empty, say $\ell = i_n$. In particular $V^{>i_n}$ is empty which implies that only $V^{i_n,0}$ is not empty inside the family $(V^{i_n,\ell})_{\ell\in\mathbb{N}}$ and that $V^{i_n,0} = V = V^{i_n} = \widetilde{V}^{i_n}$. If $n > 2$, similarly $V^{i_n,>0}$ is empty, and the only non-empty set in the family $(V^{i_n,0,\ell})_{\ell\in\mathbb{N}}$ is $V^{i_n,0,0} = V = \widetilde{V}^{i_n,0,0}$. By repeating this, it is clear that $V^{i_n,0,\ldots,0} = V = \widetilde{V}^{i_n,0,\ldots,0}$, where the number of 0s after i_n may vary from 1 to $n-2$. With exactly $n-2$ 0s, then $S_1' = \pi_1(V^{i_n,0,\ldots,0,>0}) = \emptyset$, hence $i_1 = |S_1'| = 0$, meaning that $\mathcal{L}'(\widetilde{V}) = \{(0,\ldots,i_n)\}$. In particular, the unique element $g \in G$ verifies $\textsc{lm}(g) = X_n^{i_n}$, and therefore $\min(\langle G\rangle) = \{X_n^{i_n}\}$.

Because the ideal I of vanishing polynomials on V is of dimension zero, there is a polynomial f in a Gröbner basis $\mathcal{G}_n$ of I such that $\textsc{lm}(f) = X_n^\ell$ for some $\ell > 0$. Given $\beta = (\beta_1,\ldots,\beta_{n-1}) \in \pi_{n-1}(V)$, the fiber $V[\beta]$ has cardinal i_n, and because $f(\beta, X_n) = X_n^\ell + \cdots$ must vanish on $V[\beta]$, necessarily $\ell \geq i_n$. But since $g \in I$, there exists a polynomial h in $\mathcal{G}_n$ such that $\textsc{lm}(h)|\textsc{lm}(g)$, and since $\mathcal{G}_n$ is minimal, necessarily $\textsc{lm}(h) = \textsc{lm}(f)$ implying that $\ell \leq i_n$, and henceforth $i_n = \ell$.

It remains to prove that $\min(I) = \{X_n^{i_n}\} \cup \min(\langle \mathcal{G}_{n-1}\rangle)$, more precisely that the inclusion $\subset$ holds, since the inclusion $\supset$ has been proved above. Let $f \in \mathcal{G}_n$ satisfying $\textsc{lm}(f) \in \min(I)$. Write $\textsc{lm}(f) = X_1^{a_1}\cdots X_n^{a_n}$ and let $\alpha \in \pi_{n-1}(V)$. If $a_n \geq i_n$, then necessarily $a_n = i_n$ and $a_j = 0$ for $j < n$, because $\textsc{lm}(f)$ is assumed to be in the minimal monomial basis $\min(I)$ of $\langle \textsc{lm}(I)\rangle$. Assume $a_n < i_n$. From the above, in this special case $\pi_{n-1}(V) = S_{n-1}$ and $|V[\alpha]|$ is constant equal to i_n for all $\alpha \in \pi_{n-1}(V)$. Thus if $f(\alpha, X_n) \neq 0$ then $f(\alpha, X_n) = cX_n^{a_n} + \cdots$ must vanish on $V[\alpha]$ which is not possible. Therefore $f(\alpha, X_n) = 0$ and $f \in I_{n-1}\, k[X_1,\ldots,X_n]$. But $\mathcal{G}_{n-1}$ being a Gröbner basis of this latter ideal, it follows that $\textsc{lm}(f) \in \min(\langle \mathcal{G}_{n-1}\rangle)$. This proves that $\min(I) \subset \{X_n^{i_n}\} \cup \min(\langle \mathcal{G}_{n-1}\rangle)$.

With the base case treated, the induction on $|G| = |\mathcal{L}(\widetilde{V})|c$ an be initiated to prove:

Theorem 3. *The equality $\min(I) = \min(\langle G\rangle) \cup \min(\langle \mathcal{G}_{n-1}\rangle)$ holds.*

The proof occupies the remaining of the section.

Definition 4. *Assume $|G| > 1$, and let $\mathbf{i} := \min_{\preccurlyeq} \mathcal{L}(\widetilde{V})$. Define $f := \textsc{lc}_{n-1}(g_{\mathbf{i}})$, $W := \widetilde{V}^{i_n,\ldots,i_3,i_2}$ and $W' = V \setminus W$.*

Note that $f \neq 1$, else $|G| = 1$. Since $\mathbf{i} = (i_2, i_3, \ldots, i_n) \in \mathcal{L}(\widetilde{V})$, $W := \widetilde{V}^{i_n,\ldots,i_3,i_2}$ is not empty, and since $|G| > 1$, neither is $W' = V \setminus W$.

Lemma 13. *Let $J := I(W)$ and $J' := I(W')$. These ideals satisfy the equalities $J' = I + \langle f \rangle$, and $J = I : \langle f \rangle$.*

PROOF. By Lemma 9 2., $x \in W$ verifies $\pi_k(x) \in S_k$ for all $k = 1, \ldots, n-1$, thus by Definition 3 $\pi_{n-1}(x) \in \mathcal{S}_{n-1}$. On the contrary, given $y \in W'$ $\pi_{n-1}(y) \notin \mathcal{S}_{n-1}$. Proposition 4 thus implies that $g_{\mathbf{i}}(y_1, \ldots, y_{n-1}, X_n) = 0$ and more precisely that $C_{n-1}(y_1, \ldots, y_{n-1}) = \text{LC}_{n-1}(g_{\mathbf{i}})(y_1, \ldots, y_{n-1}) = 0$ with the notations therein. It follows that $f(y_1, \ldots, y_{n-1}) = 0$ and $\pi_{n-1}(W') \subset V(f)$. This proves that $I + \langle f \rangle \subset J'$. Moreover, we have seen that $\pi_{n-1}(x)$ for $x \in V$ cancels f if and only if $y \in W'$, proving that the previous inclusion is actually an equality of ideals. The same argument shows that $f(x_1, \ldots, x_{n-1}) \neq 0$ for all $x \in W$, yielding $\pi_{n-1}(W) \cap V(f) = \emptyset$, thus $V(f) \cap V \overset{(\bullet)}{=} V \setminus W = W'$.

For the equality concerning J, recall that in general $V(I : J) = \overline{V \setminus (V(J) \cap V)}$, thus $V(I : \langle f \rangle) = V \setminus (V(f) \cap V)$, according that $f \in I$ and $V \setminus (V(f) \cap V)$ is finite hence equal to its Zariski-closure, since points are taken over the algebraic closure of k. Equality $(\bullet)$ permits then to conclude.

The Lemma above shows in particular that the ideal J and J' are co-maximal, yielding the following canonical isomorphism:

$$\begin{array}{rcl} \phi : k[X_1, \ldots, X_n]/I & \longrightarrow & k[X_1, \ldots, X_n]/J' \times k[X_1, \ldots, X_n]/J \\ p \bmod I & \longmapsto & p \bmod J' \quad , \quad p \bmod J \end{array} \tag{29}$$

Taking leading monomials defines an isomorphism of k-vector spaces, described below on the monomial bases:

$$\begin{array}{rcl} \psi : k[X_1, \ldots, X_n]/\langle \text{LM}(I) \rangle & \longrightarrow & k[X_1, \ldots, X_n]/\langle \text{LM}(J') \rangle \times k[X_1, \ldots, X_n]/\langle \text{LM}(J) \rangle \\ m \bmod \langle \text{LM}(I) \rangle & \longmapsto & m \bmod \langle \text{LM}(J') \rangle \quad , \quad m \bmod \langle \text{LM}(J) \rangle \end{array} \tag{30}$$

Remark: Let $J_{n-1} := J \cap k[X_1, \ldots, X_{n-1}]$, $J'_{n-1} := J \cap k[X_1, \ldots, X_{n-1}]$ and $I_{n-1} := I \cap k[X_1, \ldots, X_{n-1}]$. Since $f \in k[X_1, \ldots, X_{n-1}]$, it can be proved that $J'_{n-1} = I_{n-1} + \langle f \rangle$ and that $J_{n-1} = I_{n-1} : \langle f \rangle$. In particular the isomorphism ϕ and ψ defined just above, when taking relevant intersections with $k[X_1, \ldots, X_{n-1}]$, induce the following isomorphism:

$$\begin{array}{rcl} \psi' : k[X_1, \ldots, X_{n-1}]/\langle \text{LM}(I_{n-1}) \rangle & \longrightarrow & k[X_1, \ldots, X_{n-1}]/\langle \text{LM}(J'_{n-1}) \rangle \times k[X_1, \ldots, X_{n-1}]/\langle \text{LM}(J_{n-1}) \rangle \\ m \bmod \langle \text{LM}(I_{n-1}) \rangle & \longmapsto & m \bmod \langle \text{LM}(J'_{n-1}) \rangle \quad , \quad m \bmod \langle \text{LM}(J_{n-1}) \rangle \end{array} \tag{31}$$

The zero-set $W = \widetilde{V}^{i_{n-1}, \ldots, i_2}$ falls into the case of Lemma 12, hence $\min(J) = \{X_n^{i_n}\} \cup \min(J_{n-1})$. As for W', by construction $\mathcal{L}(\widetilde{W'}) = \mathcal{L}(\widetilde{V}) \setminus \{(i_2, \ldots, i_n)\}$ therefore the induction hypothesis on $|\mathcal{L}(\widetilde{V})|$ gives $\min(J') = \{X_1^{j_1} \cdots X_n^{j_n} \mid \mathbf{j} \in \mathcal{L}'(\widetilde{W'})\} \cup \min(J'_{n-1})$. In this way, $\min(J)$ and $\min(J')$ are known. The purpose of the remaining is to determine $\min(I)$ from the two known data $\min(J)$ and $\min(J')$. The strategy consists in making explicit the map (30). The following fundamental theorem plays a crucial role to this end.

Theorem 4. $\text{LM}(f)$ *is in the minimal monomial basis of* $\langle \text{LM}(J'_{n-1}) \rangle$.

PROOF. Let $Y' := \pi_{n-1}(W')$. Then $I(Y') = J'_{n-1}$. The proof of Lemma 12 shows that $i_{n-1} = 0$ if and only if $|G| = 1$, therefore we have here $i_{n-1} \neq 0$. According to Definition 2, the theorem is then equivalent to $\widetilde{Y'}^{i_{n-1}, \ldots, i_2} \neq \emptyset$ and $i_1 = |\pi_1(\widetilde{Y'}^{i_{n-1}, \ldots, i_3, >i_2})|$. Both statements follow from Proposition 3.

Corollary 5. *Let* $L := \text{LM}(I) + \langle \text{LM}(f) \rangle$ *and* $L_{n-1} := L \cap k[X_1, \ldots, X_{n-1}]$. *They satisfy the equalities* $L = \langle \text{LM}(J') \rangle$ *and thus* $L_{n-1} = \langle \text{LM}(J'_{n-1}) \rangle$.

PROOF. The inclusion $\text{LM}(J') \subset L$ is folklore. Let $\min(I) = \{n_1, \ldots, n_s, m_1, \ldots, m_t\}$ where $\min(I_{n-1}) = \{n_1, \ldots, n_s\}$ and $m_i \in k[X_1, \ldots, X_n] \setminus k[X_1, \ldots, X_{n-1}]$. By the previous theorem, $\{n_1, \ldots, n_s, \text{LM}(f), m_1, \ldots, m_t\} \subset \langle \text{LM}(J') \rangle$, yielding:

$$L \subseteq \langle n_1, \ldots, n_s, \text{LM}(f), m_1, \ldots, m_t \rangle \subseteq \langle \text{LM}(J') \rangle \subseteq L.$$

Actually, this proof works also for $\text{LM}(J'_{n-1})$ and L_{n-1} instead of $\text{LM}(J)$ and L by using only the monomials $n_1, \ldots, n_s$.

Corollary 6. *The ideals* $K := \langle \text{LM}(I) \rangle : \langle \text{LM}(f) \rangle$ *and* $K_{n-1} := K \cap k[X_1, \ldots, X_{n-1}]$ *satisfy* $K = \langle \text{LM}(J) \rangle$ *and* $K_{n-1} = \langle \text{LM}(J_{n-1}) \rangle$.

PROOF. The inclusion $\text{LM}(J) \subset K$ is elementary. Consider the onto canonical linear map:

$$\rho : k[X_1, \ldots, X_n]/\langle \text{LM}(J) \rangle \to k[X_1, \ldots, X_n]/K.$$

On the other hand, consider the isomorphism of k-vector spaces:

$$\begin{array}{rcl} \theta : k[X_1, \ldots, X_n]/\langle \text{LM}(I) \rangle & \longrightarrow & k[X_1, \ldots, X_n]/L \times k[X_1, \ldots, X_n]/K \\ m \bmod \langle \text{LM}(I) \rangle & \longmapsto & m \bmod \text{LM}(f) \ , \ m \text{ quo } \text{LM}(f) \end{array} \tag{32}$$

Comparing with ψ in (30), one sees that $\theta_2 = \rho \circ \psi_2$, (where for $i = 1, 2$ a θ_i, ψ_i are the i-th component maps of θ and ψ). Morevoer, according to Corollary 5 $\theta_1 = \psi_1$. Therefore, ρ must be an isomorphism and since it is defined as the canonical projection, it is the identity map, showing that $K = \langle \text{LM}(J) \rangle$.

To prove the equality concerning K_{n-1} is suffices to be convinced that $(\langle \text{LM}(I) \rangle : \langle \text{LM}(f) \rangle) \cap k[X_1, \ldots, X_{n-1}]$ is equal to $\langle \text{LM}((I : f) \cap k[X_1, \ldots, X_{n-1}]) \rangle$ which presents no difficulty.

Proof of Theorem 3: final argument.. The isomorphism θ in (32) shows that $\min(I) = \min(L) \setminus \{\text{LM}(f)\} \cup \{m\text{LM}(f) \mid m \in \min(K)\}$. Corollaries 5 and 6 show that $\min(L) = \min(J')$ and $\min(K) = \min(J)$ as well as $\min(L_{n-1}) = \min(J'_{n-1})$ and $\min(K_{n-1}) = \min(L_{n-1})$. Next, the discussion made before Theorem 4 tells that $\min(J) = \{X_n^{i_n}\} \cup \min(J_{n-1})$ and $\min(J') = \{X_1^{j_1} \cdots X_n^{j_n} \mid \mathbf{j} \in \mathcal{L}'(\widetilde{W'})\} \cup \min(J'_{n-1})$. Consequently,

$$\begin{array}{rl} \min(I) = \{X_1^{j_1} \cdots X_n^{j_n} \mid \mathbf{j} \in \mathcal{L}'(\widetilde{W'})\} \cup \min(J'_{n-1}) \setminus \{\text{LM}(f)\} \cup \{\text{LM}(f) X_n^{i_n}\} \cup & \\ \cup \{\text{LM}(f) m' \mid m' \in \min(J_{n-1})\}. & \end{array} \tag{33}$$

Besides, the proof of Corollary 6 also shows that the isomorphisms ψ in (30) and θ in (32) actually coincide. Therefore isomorphism ψ' in (31) is actually equal to:

$$\begin{array}{rcl} k[X_1, \ldots, X_{n-1}]/\langle \text{LM}(I_{n-1}) \rangle & \longrightarrow & k[X_1, \ldots, X_{n-1}]/L_{n-1} \times k[X_1, \ldots, X_{n-1}]/K_{n-1} \\ m \bmod \langle \text{LM}(I_{n-1}) \rangle & \longmapsto & m \bmod \text{LM}(f) \ , \ m \text{ quo } \text{LM}(f) \end{array}$$

supplying the equality $\min(I_{n-1}) = \min(J'_{n-1}) \setminus \{\text{LM}(f)\} \cup \{m\text{LM}(f) \mid m' \in \min(J_{n-1})\}$. When applied to Equality (33) this gives:

$$\min(I) = \{X_1^{j_1} \cdots X_n^{j_n} \mid \mathbf{j} \in \mathcal{L}'(\widetilde{W'})\} \cup \{\text{LM}(f) X_n^{i_n}\} \cup \min(I_{n-1}).$$

Finally, remember that $\mathcal{L}'(\widetilde{V}) = \mathcal{L}'(\widetilde{W'}) \cup \{(i_1, i_2, \ldots, i_n)\}$, and that $\text{LM}(f) = X_1^{i_1} \cdots X_{n-1}^{i_{n-1}}$, so that:

$$\min(I) = \{X_1^{j_1} \cdots X_n^{j_n} \mid \mathbf{j} \in \mathcal{L}'(\widetilde{V})\} \cup \min(I_{n-1}).$$

This is equivalent to the equality of Theorem 3 achieving its proof.

Acknowledgment

This work has benefit from several conversations with Kazuhiro Yokoyama at some early stages. I am thankful to him for these and for his encouragement.

References

[1] D. Bayer, A. Galligo, M. Stillman, Gröbner bases and extension of scalars, in: Sympos. Math. XXXIV, Cambridge Univ. Press, 1993, pp. 198–215.

[2] T. Becker, Gröbner bases versus D-Gröbner bases, and Gröbner bases under specialization, Applicable Algebra in Engineering , Communications and Computing 5 (1994) 1–8.

[3] B. Buchberger, Groebner-Bases: An Algorithmic Method in Polynomial Ideal Theory, in: N. Bose (Ed.), Multidimensional Systems Theory - Progress, Directions and Open Problems in Multidimensional Systems, 1985, Ch. 6, pp. 184–232, (Second editioin: N.K.Bose (ed.): Multidimensional Systems Theory and Application, Kluwer Academic Publisher, 2003, pp.89-128.).

[4] B. Buchberger, H. Möller, The construction of multivariate polynomials with preassigned zeros, in: Lecture Notes in Computer Science (EUROCAM'82), Vol. 144, London, UK, 1982, pp. 24–31.

[5] L. Cerlienco, M. Mureddu, From algebraic sets to monomial linear bases by means of combinatorial algorithms, Discrete Mathematics 139 (1-3) (1995) 73 – 87.

[6] X. Dahan, Size of coefficients of lexicographical Gröbner baes, in: ISSAC'09, ACM, 2009, pp. 117–126.

[7] X. Dahan, A. Kadri, E. Schost, Bit-size estimates for triangular sets in positive dimension, Journal of Complexity 28 (1).

[8] X. Dahan, É. Schost, Sharp estimates for triangular sets, in: ISSAC '04: Proceedings of the 2004 International Symposium on Symbolic and Algebraic Computation, ACM Press, 2004, pp. 103–110.

[9] B. Felszeghy, B. Ráth, L. Rónyai, The lex game and some applications, J. of Symbolic Comput. 41 (6) (2006) 663 – 681.

[10] P. Gianni, Properties of Gröbner bases under specialization, in: J. Davenport (Ed.), In Proc. of EUROCAL'87, Lecture Notes in Computer Science (378), Springer, Berlin, 1987, pp. 293–297.

[11] P. Gianni, B. Trager, G. Zacharias, Gröbner bases and primary decomposition of polynomial ideals, J. of Symbolic Comput. 6 (1988) 149–167.

[12] M. Kalkbrener, Solving systems of algebraic equations using Gröbner bases, in: J. Davenport (Ed.), In Proc. of EUROCAL'87, Lecture Notes in Computer Science (378), Springer, Berlin, 1987, pp. 282–292.

[13] D. Lazard, Ideal bases and primary decomposition: case of two variables, J. Symbolic Comput. 1 (3) (1985) 261–270.

[14] D. Lazard, Solving zero-dimensional algebraic systems, J. of Symbolic Comput. 13 (1992) 147–160.

[15] M. Lederer, The vanishing ideal of a finite set of closed points in affine space, J. of Pure and Applied Algebra 212 (2008) 1116–1133.

[16] M. G. Marinari, T. Mora, A remark on a remark by Macaulay or enhancing Lazard structural theorem, Bull. Iranian Math. Soc. 29 (1) (2003) 1–45, 85.

[17] M. G. Marinari, T. Mora, Cerlienco-Mureddu correspondence and Lazard structural theorem, Investigaciones Mathematicas 27 (2006) 155–178.